ManageEngine
Desktop Central

User Guide

Table Of Contents

INTRODUCTION **6**

USER GUIDE **8**

Software Installation 8

Installing MSI-based Applications for Users 9

Installing EXE-based Applications for Users 10

Installing MSI-based Applications for Computers 11

Installing EXE-based Applications for Computers 12

Uninstalling MSI-based Applications for Users 13

Uninstalling EXE-based Applications for Users 14

Uninstalling MSI-based Applications for Computers 15

Uninstalling EXE-based Applications for Computers 16

Patch Management 17

Patch Management Architecture 18

Patch Management Life Cycle 20

Scan Systems for Vulnerability 22

Installing Missing Patches 23

Patch Views 24

Viewing Applicable Patches 25

Viewing Latest Patches 27

Viewing Missing Patches 28

Viewing Installed Patches 29

Viewing Supported Patches 30

Viewing Healthy Systems 31

Viewing Vulnerable Systems 32

Viewing Highly Vulnerable Systems 33

Viewing Patch Reports 34

Viewing Vulnerable Systems Report 35

Viewing Vulnerable Patches Report 36

Viewing Supported Patches Report 37

Hardware and Software Inventory 38
Hardware / Software Inventory and Asset Management 38
Software Metering 39
Viewing Computer Details 41
Viewing Hardware Details 42
Viewing Software Details 43
Viewing Inventory Alerts 45
Viewing Inventory Reports 46
Hardware Inventory Reports 47
Software Inventory Reports 49
Software License Compliance Reports 51
Windows Tools 52
System Tools 53
Creating and Scheduling Tasks 54
Viewing and Modifying the Tasks 58
Viewing Task History 59
Remote Desktop Sharing 60
Remote Desktop Sharing - Pre-requisites 61
Connecting to Remote Desktop 63
Troubleshooting Tips 65
Wake on LAN 67
Remote Shutdown Tool 70
Windows Configurations 75
User Configurations 76
Configuring Alerts 77
Executing Custom Scripts 78
Configuring Display Settings 80
Mapping Network Drives 82
Setting Environment Variables 84
Managing Files and Folders 86
Redirecting User-Specific Folders 89
Installing Software - MSI & EXE Packages 91
Configuring Internet Explorer Settings 95
Configuring IP Printer 97
Launching Applications 99
Displaying Message Box 101

Configuring MS Office Settings 102
Configuring Outlook Settings 104
Setting Path 107
Managing Permissions 108
Configuring Power Options 112
Configuring Registry Settings 115
Securing USB Devices 119
Configuring Security Policies 121
Configuring Shared Printer 123
Managing Shortcuts 125
Computer Configurations 128
Redirecting Common Folders 129
Executing Custom Scripts 131
Setting Environment Variables 133
Managing Files and Folders 135
Configuring Windows XP Firewall 138
Configuring General Computer Settings 140
Managing Windows Local Groups 141
Installing Patches 143
Installing Software - MSI & EXE Packages 145
Installing Windows Service Packs 149
Configuring IP Printer 151
Launching Applications 153
Displaying Legal Notices 155
Displaying Message Box 156
Setting Path 157
Managing Permissions 158
Configuring Registry Settings 162
Securing USB Devices 165
Scheduling Tasks 166
Configuring Security Policies 169
Managing Shortcuts 171
Configuring Windows Services 174
Managing Windows Local Users 176
Configuring Collections 180
Defining Targets 181
Managing Configurations and Collections 185

Viewing System Uptime Report 187
Viewing Configuration Reports 188
Configuration Templates 189
Computer Configuration Templates 191
User Configuration Templates 194
User Logon Reports 195
Viewing User Logon Reports 196
General Reports 197
Usage Reports 198
History Reports 199
Active Directory Reports 200
Active Directory User Report 201
Active Directory General User Reports 202
User Account Status Reports 204
Password Based User Reports 206
Privileged User Accounts 207
Logon Based User Reports 208
Active Directory Computer Reports 209
General Computer Reports 210
Server Based Reports 212
Computer OS Based Reports 213
Active Directory Group Reports 214
Active Directory General Group Reports 215
Active Directory Group Type Reports 217
Member Based Reports 218
Active Directory Organization Unit Reports 220
Active Directory General OU Reports 221
OU Child Based Reports 222
Active Directory Domain Reports 223
General Domain Reports 224
Container Based Reports 225
Active Directory GPO Reports 226
General GPO Reports 227
GPO Link Based Reports 228
Inheritance Based Reports 229

GPO Status Based Reports 230
Special GPO Reports 232
Custom Reports 233
Creating Custom Reports 234
Custom Query Report 235
Making Help Desk Requests 237
APPENDIX 238
Interpreting Error Messages 239
FAQs 242
Security Policies 245
Security Policies - Active Desktop 246
Security Policies - Desktop 248
Security Policies - Control Panel 249
Security Policies - Explorer 251
Security Policies - Internet Explorer 253
Security Policies - Network 256
Security Policies - System 258
Security Policies - Task Scheduler 260
Security Policies - Windows Installer 261
Security Policies - Start Menu and Taskbar 262
Security Policies - Microsoft Management Console 264
Security Policies - Computer 268
Windows System Tools 269
Check Disk Tool 270
Disk Cleanup Tool 271
Disk Defragmenter Tool 272
Data Backup and Restore 273
Data Restore 274
Dynamic Variables 275
Limitations 277
Glossary 279

Introduction

ManageEngine® Desktop Central

Desktop administration is a never-ending job. Configuration requests ranging from simple Drive Mapping configuration to software installation keep the administrators on their toes. With increasing requests and a growth in the number of desktop, it becomes more difficult to keep up with escalating demand on limited manpower.

Desktop Central enables configuring and managing desktop from a single point. With the pre-defined configuration options, administrators can perform almost all the regular desktop administration / management activities with ease. The ability to execute custom script gives complete administration control over the desktop. The Web-based user interface allows for applying the configuration to a single or group of desktop using a powerful filtering capability.

Desktop Central ensures that the configurations are applied to the desktop and the status is made available to the administrator to provide an end-to-end configuration experience.

In addition to the remote configuration options, it also provides you with an automated patch management system that helps you to manage and apply Windows patches and hot fixes.

The Inventory Management module provides the hardware and software details of the devices in the network. In enables you to manage the software licenses and detect any unauthorized software that are being used.

Remote Desktop Sharing enables you to gain access to a desktop in the network to be controlled remotely.

Desktop Central provides the complete history of the configurations applied to the users, computers, and by configuration types in the form of reports that can be used for auditing the deployed configurations.

In addition to the configurations reports, it also provides Active Directory reports for Sites, Domains, Organization Units, Groups, Computers, etc., which gives you a complete visibility into the Active Directory.

The User Logon Reports provides an up-to-date user logon details like the logon time, logoff time, logon computer, reported logon server, etc. It maintains the history of the logon details that can be used for auditing purposes.

The following sections will help you to get familiar with the product:

- Getting Started: Provides you the details of system requirements, product installation and startup.
- Configuring Desktop Central: Helps you to customize our product to suit your working environment.
- Windows Configurations: A step-by-step guide to define and deploy configurations to remote Windows users and computers.

- Configuration Templates: Provides the details of configuration templates and helps you to define configurations from Templates
- Software Installation: Helps you to install Windows software to the users and computers of the domain from remote.
- Patch Management: Details the steps involved in managing the Windows Patches and hot fixes. It helps you to automate the patch management process.
- Hardware and Software Inventory: Guides you to collect the hardware and software inventory details of your network and view the reports.
- Active Directory Reports: Helps you to view the reports of the Active Directory components.
- Windows Tools: Provides the list of Windows tools like Preventive Maintenance Tools, Remote Tools, etc., and the steps in using them.
- User Logon Reports: Helps you get an up-to-date- details of the user logon and history.
- Appendix: This section includes, Interpreting Error Messages, Knowledge Base, FAQs, Known Issues and Limitations of Desktop Central, and Glossary.

User Guide

Software Installation

Desktop Central enables remote software deployment and distribution to the users and computers of the Windows network. This web-based software deployment configuration helps administrators to install software from a central point. It supports deploying both MSI and EXE based applications that can be installed in a silent mode.

Software Distribution Features

- Supports installing both MSI and EXE based applications.
  - Supports Install, Uninstall, Assign and Redeploy options for MSI based applications.
  - Supports Install and Uninstall options for EXE based applications.
- Ability to schedule software installations.
  - Install Software at a specified time
  - Install Software either during or after startup of the computer.
- Option to install the application as a specific-user using the **Run As** option.
- Supports executing pre-installation scripts/commands prior to installation and abort if not successful.
- Option to copy the installables to the client computers before installing the software.
- Ability to create package repository. The packages created once can be reused any number of times to install or uninstall the software.

The following links guides you to install software from remote using Desktop Central:

- Managing Software Packages
- Installing MSI-based Applications for Users
- Installing EXE-based Applications for Users
- Installing MSI-based Applications for Computers
- Installing EXE-based Applications for Computers
- Uninstalling MSI-based Applications for Users
- Uninstalling EXE-based Applications for Users
- Uninstalling MSI-based Applications for Computers
- Uninstalling EXE-based Applications for Computers

Installing MSI-based Applications for Users

To install an MSI application to the users, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install Completely**, **Assign**, or **Redeploy** as the case may be. If you select the **Assign** option, the application will be installed only when the user tries to open the application for the first time.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the users to whom the software has to be installed.
10. Click **Deploy**.

Installing EXE-based Applications for Users

To install an EXE application to the users, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the users to whom the software has to be installed.
10. Click **Deploy**.

Installing MSI-based Applications for Computers

To install an MSI application to the computers, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install Completely**, **Assign**, or **Redeploy** as the case may be. If you select the **Assign** option, the application will be installed only when the user tries to open the application for the first time.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the computers in which the software has to be installed.
10. Click **Deploy**.

Installing EXE-based Applications for Computers

To install an EXE application to the computers, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the computers in which the software has to be installed.
10. Click **Deploy**.

Uninstalling MSI-based Applications for Users

To uninstall an MSI application for users, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the user objects from which the software has to be uninstalled.
10. Click **Deploy**.

Uninstalling EXE-based Applications for Users

To uninstall an EXE application for the user objects, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the user objects from which the software has to be uninstalled.
10. Click **Deploy**.

Uninstalling MSI-based Applications for Computers

To uninstall an MSI application from the computer objects, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the computer objects from which the software has to be uninstalled.
10. Click **Deploy**.

Uninstalling EXE-based Applications for Computers

To uninstall an EXE application from the computer objects, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the computer objects from which the software has to be removed.
10. Click **Deploy**.

Patch Management

The steady increase in network vulnerabilities and the sheer volume of software patches that fix these threats, over the years; has created a need for strict and efficient patch management in enterprises to avoid business downtime and to secure themselves against mishaps due to attacks.

The best way to address this problem, is to have a systematic, automated and affordable solution that is robust and manages patches effectively. Desktop Central with its Patch Management module provides the system administrators the ability to respond to computer threats in quick time. All this in compliance to the patch management life cycle and with a fresh perspective to network security.

Patch Management Features

- Uses a hosted Patch Database at Zoho Corp. site to assess the vulnerability status of the network.
- Complete automated Patch Management Solution from detecting the vulnerabilities to deploying the patches.
- Patch based deployment - Deploy a patch to all the affected systems
- System based patch deployment - Deploy all the applicable patches for a system
- Automatic handling of patch interdependencies and patch sequencing
- Reports on System vulnerabilities, Patches,OS, etc.
- Provides an update of the patch deployment status

Follow the links to learn more,

- Patch Management Architecture
- Patch Management Life Cycle
- Setting up Patch Management Module
- Scan Systems for Vulnerability
- Viewing Applicable Patches
- Viewing Latest Patches
- Viewing Missing Patches
- Installing Missing Patches
- Viewing Installed Patches
- Viewing Supported Patches
- Viewing Healthy Systems
- Viewing Vulnerable Systems
- Viewing Highly Vulnerable Systems
- Viewing Patch Reports

Patch Management Architecture

- The Patch Management Architecture
- How it Works

The Patch Management Architecture

The Patch Management consists of the following components:

- External Patch Crawler
- Central Patch Repository
- Desktop Central Server

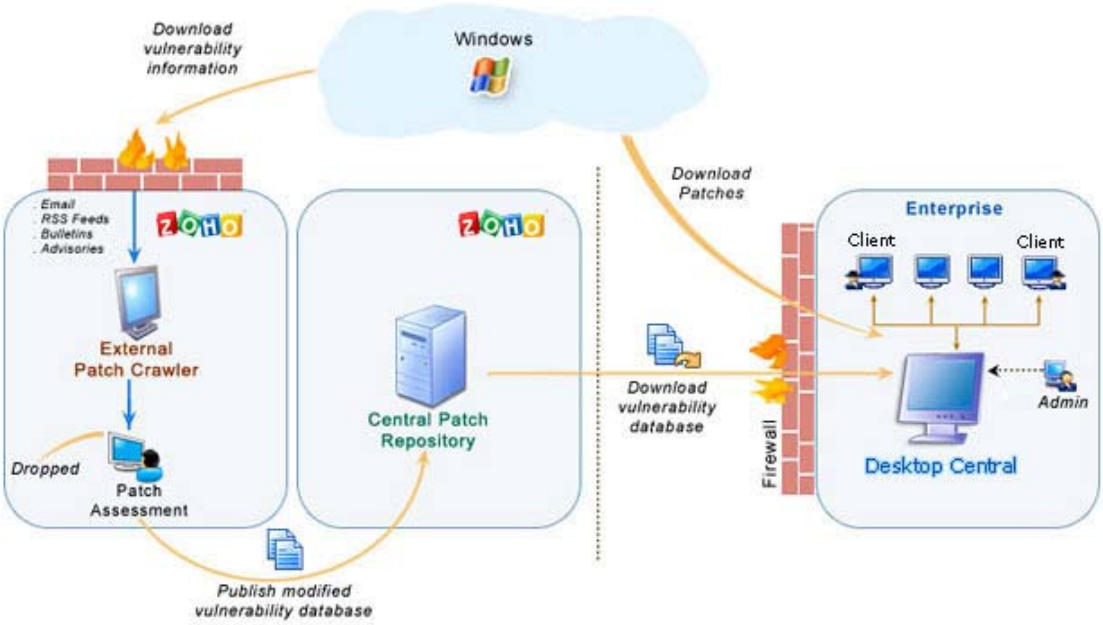


Fig: Patch Management Architecture

The *External Patch Crawler* resides at the Zoho Corp. site and repeatedly probes the internet to draw vulnerability information from the Microsoft website.

Patch download, assessment for patch authenticity and testing for functional correctness is also carried out at this site. The final analysis and data are correlated to obtain a consolidated vulnerability database which serves as a baseline for vulnerability assessment in the enterprise. The modified vulnerability database is then published to the Central Patch Repository for further use. The whole process of information gathering, patch analysis and publishing the latest vulnerability database occurs periodically.

The *Central Patch Repository* is a portal in the Zoho Corp. site, which hosts the latest vulnerability database that has been published after a thorough analysis. This database

is exposed for download by the Desktop Central server situated in the customer site, and provides information required for patch scanning and installation.

The *Desktop Central Server* is located at the enterprise (customer site) and subscribes to the Central Patch repository, to periodically download the vulnerability database. It scans the systems in the enterprise network, checks for missing and available patches against the comprehensive vulnerability database, downloads and deploys missing patches and service packs, generates reports to effectively manage the patch management process in your enterprise.

How it Works?

Patch Management using Desktop Central is a simple two-stage process:

- Patch Assessment or Scanning
- Patch Download and Deployment

Patch Assessment or Scanning

Desktop Central periodically scans the systems in your windows network to assess the patch needs. Using a comprehensive database consolidated from Microsoft's bulletins, the scanning mechanism checks for the existence and state of the patches by performing file version checks, registry checks and checksums. The vulnerability database is periodically updated with the latest information on patches, from the Central Patch Repository. The scanning logic automatically determines which updates are needed on each client system, taking into account the operating system, application, and update dependencies.

On successful completion of an assessment, the results of each assessment are returned and stored in the server database. The scan results can be viewed from the web-console.

Patch download and deployment

On selecting the patches to be deployed, you can a trigger a download or a deploy request. At first the selected patches are downloaded from the internet and stored in a particular location in the Desktop Central server. Then they are pushed to the target machines remotely, after which they are installed sequentially.

See Also: Patch Management Life Cycle, Setting Up Patch Management Module, Scan Systems for Vulnerability, Patch Reports

Patch Management Life Cycle

Desktop Central Patch Management module consists to the following five stages:

1. Update Vulnerability Details from Vendors
2. Scan the Network
3. Identify Patches for Vulnerabilities
4. Download and Deploy Patches
5. Generate Status Reports

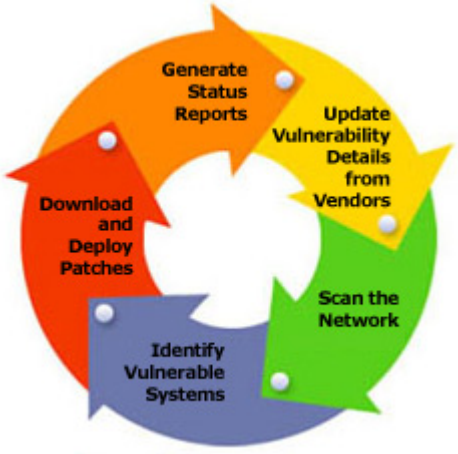


Fig: Patch Management Life Cycle

Update Vulnerability Details from Vendors

- Be up-to-date with the latest patch related information from the various sources.
- Download patches and run extensive tests to validate the authenticity and accuracy of patches

Scan the Network

- Discover and identify the systems in the network based on the defined Scope of Management.

Identify Patches for Vulnerabilities

- Assess the vulnerabilities in the systems periodically.
- Analyze what patches are missing and what are installed.

Download and Deploy Patches

- Download the required patches from the vendor site.
- Deploy patches in the missing systems.
- Verify and validate the accuracy of patch installation

Generate Status Reports

- Generate reports of various patch management tasks.
- Monitor the patching progress in the enterprise.

See Also: Patch Management Architecture, Setting Up Patch Management Module, Scan Systems for Vulnerability, Patch Reports

Scan Systems for Vulnerability

Desktop Central periodically scans the systems in your Windows network, to determine the vulnerable systems/applications. The latest status of the scan and the scan reports can be accessed by clicking the **Scan Status** link available under the **Patch Mgmt** tab. The following details are shown here:

- **Computer Name**: The DNS name of the computer being scanned.
- **OS Name**: The operating system of the computer being scanned.
- **Agent Status**: Specifies whether the agent is installed in the system or not.
- **Agent Version**: Specifies the agent version.
- **Last Scan Status**: The status of the previous scan.
- **Last Scan Time**: Time at which the scan was performed. Clicking this link will open the Vulnerable Systems Report for that system.

It also provides a graphical representation of the scanned systems. You can initiate the scan for any specific system by selecting the system and clicking the Scan Now button or can initiate the scan for all the systems by clicking the Scan All button.

To reschedule the scan, refer to the Configure Patch Scan Mode and Scan Interval

See Also: Patch Management Architecture, Patch Management Life Cycle, Setting Up Patch Management Module, Patch Reports

Installing Missing Patches

After identifying the missing patches in your network, the next step is to install the patches to fix the vulnerability. You can install the patches using Desktop Central by any of the following ways:

From the Applicable and Missing Patches Views

- By clicking the  icon from the action column of the patches.
- By selecting the patches and clicking the **Install Patches** button.

Both the above options will open the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

From the Latest and All Supported Patches Views

By selecting the patches and clicking the **Install Patches** button, opens the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

From the All Managed, Vulnerable, and Highly Vulnerable Systems Views

1. Click the Missing Patches link to view the missing patches of that system.
2. Select the patches and click the Install Patches button.

This opens the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

From the Install Patches Configuration

Like any other configuration, you can manually define a configuration for installing patches in computers.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Patch Views

- Viewing Applicable Patches
- Viewing Latest Patches
- Viewing Missing Patches
- Viewing Installed Patches
- Viewing Supported Patches
- Viewing Healthy Systems
- Viewing Vulnerable Systems
- Viewing Highly Vulnerable Systems

Viewing Applicable Patches

Viewing Applicable Patches

The Applicable Patches view provides the details of the patches that affects the applications/systems in your network. The patch list also include the patches that are already installed in your network.

To view the list of the applicable patches, click the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The network snapshot depicts the health and patch status of the systems in the network.

The details of the applicable patches shown in the tabular form include:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet.
- **Action**: You can initiate the following actions by clicking the icons:
  - - Scan the systems that do not have the patch installed to reconfirm the status.
  - - To deploy the patch on the missing systems. This opens the Installing Patches Configuration with the patch added to the configuration; select the targets and deploy.

Installing Patches

You can install the patches in any of the following ways:

- by clicking the icon of a patch
- by selecting the patches to be installed and by clicking the **Install Patches** button.

Both the above operations, will open the Installing Patches Configuration, with the selected patches added. Select the targets and deploy the configuration.

Bulletin Details

Bulletin details includes the following:

- Bulletin ID: The advisory article provided by the vendor which contains information about the vulnerability and patch availability.
- Posted On: The date of release of this bulletin.
- Updated On: The date of last update to this bulletin.
- FAQ Page: Links to the FAQ section in the Microsoft site for this bulletin.
- Q Number: Links to the knowledge base article available in the Microsoft web site.
- Issue: Details of the related issue.
- Bulletin Summary: A brief summary of the bulletin.
- Patch Details: The name of the patch and the affected products.

Patch Details

The following patch details are shown:

- Patch ID: A unique reference ID in Desktop Central for every patch
- Patch Name: The name of the patch
- Bulletin ID: The Bulletin ID pertaining to this patch
- MS Knowledge Base: The knowledge base article corresponding to this patch.
- Severity: The severity of the patch.
- Reboot: Specifies whether a system reboot is required on installing the patch.
- Download Status: Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- Location Path: The complete download URL of the patch.
- Superseding Bulletin ID: Refers to the Bulletin ID pertaining to the patch that has taken its place.
- CVEID:
- BugTraq ID:

It also provides the details of the changes made to the files and registries on installing this patch.

See Also: Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Latest Patches


Viewing Latest Patches

The Latest Patches view lists the details of the patches pertaining to the recently released Microsoft Bulletins.

To view the Latest Patches, select the Latest Patches link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The following details of the patches are displayed:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Download Status**: Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Reboot**: Specifies whether the patch installation requires a system reboot or not.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.

You can initiate the following actions from here:

- **Download**: Selecting the required patches and clicking Download will download the patch from the vendor site and make it available in the Desktop Central's Patch Repository for deployment.
- **Install Patches**: Selecting the required patches and clicking Install Patch, will open the Install Patch Configuration page from where you can select the targets and deploy.

See Also: Viewing Applicable Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Missing Patches

Viewing Missing Patches

The Missing Patches view provides the details of the patches that affects the applications/ systems in your network, which are not installed.

To view the list of the missing patches, click the **Missing Patches** link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The severity of the missing patches are depicted in a graph.

The details of the missing patches shown in the tabular format include:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet.
- **Action**: You can initiate the following actions by clicking the icons:
  - - Scan the systems that do not have the patch installed to reconfirm the status.
  - - To deploy the patch on the missing systems. This opens the Installing Patches Configuration with the patch added to the configuration; select the targets and deploy.

Installing Patches

You can install the patches in any of the following ways:

- by clicking the icon of a patch
- by selecting the patches to be installed and by clicking the **Install Patches** button.

Both the above operations, will open the Installing Patches Configuration, with the selected patches added. Select the targets and deploy the configuration.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Installed Patches

Viewing Installed Patches

The Installed Patches view provides the details of the patches that are installed in your network.

To view the list of the installed patches, click the **Installed Patches** link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The severity of the installed patches are depicted in a graph.

The details of the missing patches shown in the tabular format include:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed.

To install multiple patches, select the patches and click Install Patches, which will open the Patch Configuration from where you can select the targets and deploy.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Supported Patches

Viewing Supported Patches

The All Supported Patches view provides the details of all the patches released by Microsoft Corporation that are supported by Desktop Central.

To view the supported patches, click the **All Supported Patches** link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack. The following details are shown:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Download Status**: Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Reboot**: Specifies whether the patch installation requires a system reboot or not.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Superceded By**: Indicates that the patch is outdated and have another patch that is more recently released and has taken its place.

This information is retrieved from the Central Patch Repository that resides at the Zoho Corp.'s site periodically.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Healthy Systems

Viewing Healthy Systems

Healthy systems are those that have all the security patches installed. To view the healthy systems in your network, click the **Healthy Systems** link under the **Patch Mgmt** tab.

The following details about the healthy systems are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Vulnerable Systems

Viewing Vulnerable Systems

Vulnerable systems are those that do not have one or more Moderate/Low rated patches installed. To view the Vulnerable systems in your network, click the **Vulnerable Systems** link under the **Patch Mgmt** tab.

The following details about the vulnerable systems are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Highly Vulnerable Systems

Viewing Highly Vulnerable Systems

Viewing Highly Vulnerable Systems

Highly Vulnerable systems are those that do not have one or more Critical/Important rated patches installed. To view the highly vulnerable systems in your network, click the **Highly Vulnerable** link under the **Patch Mgmt** tab.

The following details about the highly vulnerable systems are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems

Viewing Patch Reports

Viewing Patch Reports

The Patch Reports provides you with detailed information about the vulnerable systems in your network and the patch details to fix the vulnerability. Desktop Central determines the vulnerability of the systems by periodic scanning to check whether the applicable patches have been installed. The following reports helps you to check your network vulnerability:

- Vulnerable Systems Report
- Vulnerable Patches Report
- Supported Patches Report

Viewing Vulnerable Systems Report

Viewing Vulnerable Systems Report

The Vulnerable Systems Report provides you a snapshot of the healthy and vulnerable systems in your network.

To view the report, click the **Vulnerable Systems Report** link available under the **Reports** tab. The details of the managed systems and their related patches are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

Application and Patch Summary Report

Clicking the system count from the Vulnerable Systems Report, provides you the application-wise patch details for that system with their state like installed, missing, informational, obsolete, etc.

See Also: Viewing Vulnerable Patches Report, Viewing Supported Patches Report, Viewing Task Status Report

Viewing Vulnerable Patches Report

Viewing Vulnerable Patches Report

The Vulnerable Patches Report provides you the details of the patches that are applicable to your network and the affected systems. By default, it lists the details of the patches released in the current month. You have an option to select a different period or to specify a custom period and generate the report.

To view the report, click the **Vulnerable Patches Report** link available under the **Reports** tab. The following details are shown here:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed. Click this link to view the details.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed. Click this link to view the details.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet. Click this link to view the details.

See Also: Viewing Vulnerable Systems Report, Viewing Supported Patches Report, Viewing Task Status Report

Viewing Supported Patches Report

Viewing Supported Patches Report

The Supported Patches Report provides the details of all the patches released by Microsoft Corporation irrespective of whether it is related to your network or not. When you plan to upgrade the systems in your network by installing the latest applications, you can sneak through this report to check whether any updates are available for the application.

By default, it lists the details of the patches released in the current month. You have an option to select a different period or to specify a custom period and generate the report.

To view the report, click the **Supported Patches Report** link available under the **Reports** tab. The following details of the patches are shown here:

- **Patch ID**: A unique reference ID in Desktop Central for every patch.
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**:The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Reboot**: Specifies whether the patch installation requires a system reboot or not.

See Also: Viewing Vulnerable Systems Report, Viewing Vulnerable Patches Report, Viewing Task Status Report

Hardware and Software Inventory

Hardware / Software Inventory and Asset Management

The Inventory module provides comprehensive details about the hardware and software details of the Windows systems in the network that helps in Asset Management.

Desktop Central periodically scans the network to collect the hardware and software asset details from each Windows desktop. The Hardware inventory details include information like, memory, operating system, manufacturer, device types, peripherals, etc. The Software inventory provides details of the software detected in the network grouped by volume and software vendors. It also provides the license compliance details of the software and software metering.

Scanning the Windows systems for inventory assets can be scheduled to have an up-to-date information. Alerts are generated to notify any specific events like a new hardware/software detected, license not compliant, etc. The comprehensive reports helps you to view the details in few clicks.

Inventory Management Features

- Complete Hardware and Software Inventory.
- Scan the systems periodically to collect the hardware and software details.
- Manage Software Licenses.
- Detect Prohibited Software in the network.
- Provides software usage statistics.
- Alert on specific events.
- Comprehensive reports on hardware, software inventory and license compliance.

Follow the links to learn more,

- Software Metering
- Viewing Computer Details
- Viewing Hardware Details
- Viewing Software Details
- Viewing Inventory Alerts
- Viewing Inventory Reports

Software Metering

Software Metering helps you to monitor the software usage in your organization. Desktop Central Software Metering and Software Inventory helps you to achieve the following:

- Get the list of software used by each user
- Get the list of prohibited software used in your network
- Get the software usage details, which helps you to plan software purchases
- Get the software license compliance status, which helps you to plan additional license purchases or cancel unused licenses.

Software License Management

Desktop Central provides an option to input the license details of the commercial software used in the network. These details are used in arriving at the software compliance status for each software installed in the network. The software compliance status helps to know software licensing details like the number of software licenses purchased, the number of software licenses that are currently in use and the number of software licenses that are remaining. When the number of software licenses that are used exceeds the actual software licenses purchased, it means that you are not compliant and need to purchase more licenses to become compliant.

The Software License Management provides the following compliance status:

- **Under-Licensed**: When the software copies in use is greater than the copies purchased. This means that you do not have adequate licenses and need to purchase more licenses to become compliant.
- **Over-Licensed**: When the software copies in use is less than the copies purchased. This means that you have purchased more licenses than you actually use.
- **Compliant**: When the software copies in use is almost same as the copies purchased.

Prohibited Software Details

Every organization will have a set of software that are prohibited to be used in accordance with the company policies. Detecting such prohibited software will help in tackling the compliance issues that might arise later. Desktop Central provides an option to add the list of prohibited software of your company. When any such software is detected it can be configured to be notified through an email to take necessary action.

Software Usage Statistics

It is important to monitor the software usage statistics and record them. Desktop Central provides the details of all the software installed in the network with the total number of copies with the usage details of each software like, Frequently Used, Occasionally Used, or Rarely Used. This will give a complete picture of the used and unused software in the network. This helps to decide on the software purchases and renewals based on the

actual usage. The savings on the license renewal cost can be huge when unused or very rarely used software are known well before the renewal time.

The Software Usage can be any of the following:

- **Frequently Used**: Refers to the software that are used more often.
- **Occasionally Used**: Refers to software that are less frequently used.
- **Rarely Used**: Refers to the software that are rarely being used.

Software Metering Reports

The Software Inventory Reports and the Software Compliance Reports helps the administrators to get the Software Metering details and subsequently helps to decide on the software purchases and renewals.

Viewing Computer Details

The Computers view provides the details of the computers and their operating systems.

To view the computers, select the **Inventory** tab and click the **Computers** link. It also provides a graphical representation of the computers by their operating systems. The table below provides the following details of the computers:

- **Computer Name**: The DNS name of the computer
- **Operating system**: The operating system of the computer
- **Service Pack**: The service pack version of the operating system
- **Version**: The operating system version.
- **Virtual Memory**: Total virtual memory in kilobytes.
- **Free Virtual Memory**:Total virtual memory in kilobytes that is currently unused and available.
- **Visible Virtual Memory**:Total physical memory that is available to the operating system.
- **Free Visible Memory**: Total physical memory that is currently unused and available.

You can use the **Column Chooser** to select the columns to view.

Viewing Hardware Details

The Hardware view provides the details of the hardware detected in the scanned systems.

To view the hardware details, select the **Inventory** tab and click the **Hardware** link. It provides the following details:

- **Hardware Name**: Name of the hardware device.
- **Hardware Type**: Type of the hardware like processor, keyboard, port, etc.
- **Manufacturer**: Name of the manufacturer of that hardware device.
- **Number of Items**: Total number of items available in the scanned system. To get the details of number of copies available in each system, click the number of items.

You can use the **Column Chooser** to select the columns to view.

Viewing Software Details

The Software Inventory view provides the details of the software detected in the scanned systems.

To view the software inventory details, select the **Inventory** tab and click the **Software** link. You can filter the view by Software Type, Access Type, or License Compliance status using the **Filter** option. It provides the following details:

- **Software Name**: Name of the software.
- Version: The version of the software.
- **Software Type**: Can be either commercial or non-commercial. Use the **Move To** option to specify the software type.
- **Purchased**: Number of copies purchased. This information has to be provided by clicking the **Add / Modify License** button or from Manage Software Licenses.
- **Installed**: Number of copies installed.
- **Remaining**: Number of licenses remaining.
- **Compliant Status**: The license compliance status of the software. The status is arrived based on the license count specified using the **Add / Modify License** button or from Manage Software Licenses and is not applicable for non-commercial software.
- **Access Type**: Can be either Allowed or Prohibited. To add/remove software to the prohibited links, use the **Move To** option or from Configure Prohibited Software.
- Vendor: The software vendor.
- **Licensed To**: Refers to the person or the company to whom the software is licensed.
- **Purchased Date**: Date of purchase of license.
- **License Expiry Date**: Date of license expiry.
- **Remarks**: Remarks, if any.

You can use the **Column Chooser** to select the columns to view.

To Add License Details

1. Select the software from the table and click **Add / Modify License**. This opens the Add / Modify License view.
2. The manufacturer and the software version details are pre-filled and cannot be modified.
3. Specify the number of licenses purchased.
4. Specify the purchase and expiry date in the respective fields (optional).
5. Click **Add License**.

To Specify Software and Access Type

1. Select the software from the table and choose the access or the software type from the Move To combo box. You can select multiple software and choose the required option.
2. Click **OK** to confirm.

To Assign Software to a specific Category

1. Select the software from the table and choose a category from the Assign To Category combo box. You can select multiple software and assign them to a category.
2. Click **OK** to confirm.

Note: When you assign a software that was earlier assigned to a different category to a new category, it gets automatically disassociated from the previous category. This means that you cannot have the same software in two different categories simultaneously.

Viewing Inventory Alerts

Desktop Central generates Email Alerts to notify the following:

1. When a new hardware is detected in the network
2. When a new software is detected in the network
3. Non Compliance of software licensing policy, i.e., the license is inadequate and have to purchase more licenses to be compliant
4. When a prohibited software is detected in the network.

Based on the alert configuration, alerts are generated. You can view the alerts selecting the **Inventory** tab and clicking the **Alerts** link from the left pane.

You can filter the view based on the Alert Type, which can be any of the following:

- Hardware Added
- Hardware Removed
- Allowed Software Installed
- Allowed Software Uninstalled
- Prohibited Software Installed
- Prohibited Software uninstalled
- Software Under-Licensed
- License Expired
- Prohibited Software Identified
- New Computer Identified

Viewing Inventory Reports

Viewing Inventory Reports

Desktop Central provides various out-of-the-box inventory reports to view the software and hardware inventory details of the systems in the network. It also provides reports for verifying the license compliance and software metering.

- Hardware Inventory Reports
- Software Inventory Reports
- Software Compliance Reports

Hardware Inventory Reports

Hardware Inventory Reports

- Computers by OS
- Computers by Manufacturer
- Computers by Memory
- Computers by Age
- Computers by Device Type
- Computer by Disk Usage

Computers by OS

Provides the details of the computers by their operating system. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by OS** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Manufacturer

Provides the details of the computers by their manufacturer. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Manufacturer** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Memory

Provides the details of the computers by their RAM size. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Memory** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Age

Provides the details of the computers by their year of manufacturing. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Age** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Device Type

Provides the details of the computers based on their type like, Laptop, Portable, Desktop etc. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Device Type** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computer by Disk Usage

Provides the details of the computers along with their total and free hard disk space. You can filter the view by domain ot by specifying the disk usage criteria. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computer by Disk Usage** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Software Inventory Reports


Software Inventory Reports

- Software by Manufacturer
- Recently Installed Software
- Prohibited Software
- Software Usage by Computer
- Software Product Keys

Software by Manufacturer

Provides the details of the software installed in the scanned systems based on their vendors along with the total number of copies installed. Clicking the copies count will show the computers that have the software installed. You can filter the view by selecting a vendor from the combo box.

To view the report, select the **Inventory** tab and choose the **Software by Manufacturer** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Recently Installed Software

Provides the list of software installed recently. You can choose to select a pre defined period or provide a custom period to get the software list.

To view the report, select the **Inventory** tab and choose the **Recently Installed Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Prohibited Software

Provides the list of prohibited software detected in the network.

To view the report, select the **Inventory** tab and choose the **Prohibited Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Usage by Computer

Provides the list of software and their usage statistics in individual computers.

To view the report, select the **Inventory** tab and choose the **Software Usage by Computer** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Product Keys

Provides the list of Product Keys that were used for installing the software. The Product Keys can be identified for the following software:

1. Adobe Photoshop
2. Macromedia Dreamweaver
3. Macromedia Flash
4. Microsoft Office
5. Microsoft SQL Server
6. Microsoft Visual Studio

To view the report, select the **Inventory** tab and choose the **Software Product Keys** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software License Compliance Reports

 **Software License Compliance Reports**

- Software License Compliance Report
- Software Licenses to be Renewed

Software License Compliance Report

Provides the details of the commercial software with their software license compliance status. The software license compliance status is determined based on the input provided in the Manage Software Licenses.

To view the report, select the **Inventory** tab and choose the **License Compliance Report** link available under License Reports category by hovering the mouse over the **Inventory Reports**

Software Licenses to be Renewed

Provides the list of software whose licenses have to be renewed shortly. You can choose the time period from the combo box. You can also view the software licenses that has already expired by selecting the appropriate option. Based on the Software Metering and the usage statistics, you can decide whether to renew the licenses or not.

To view the report, select the **Inventory** tab and choose the **Licenses to be Renewed** link available under License Reports category by hovering the mouse over the **Inventory Reports**

Windows Tools

Desktop Central provides various windows tools that can be run on the network system simultaneously. This section guides you through the purpose and the process of accessing these tools. The Windows Tools include the following:

- System Tools
- Remote Desktop Sharing
- Wake on LAN Tool
- Remote Shutdown Tool

To access these tools, select the Tools tab from the Desktop Central Client and click on the respective tool.

System Tools

Windows System Tools

Desktop Central provides various system tools, such as Disk Cleaner, Disk Checker, and Disk Defragmenter, that can be run on the multiple computers simultaneously. This section guides you through the process of creating and scheduling tasks to run these tools and to view the status history of the tasks that are executed. Follow the links to learn more:

- Creating and Scheduling Tasks
- Viewing and Modifying the Tasks
- Viewing the Task History

Creating and Scheduling Tasks

Creating and Scheduling Tasks

To create and schedule a task to run the Windows system tools in multiple computers, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled. Click the Add Task button to create a new task. This opens the Add Task Wizard and follow the instructions as explained below:

Step 1: Define Task

1. Provide a name and description for the task.
2. Select the tools that you wish to run and click Next.
3. Based on the tool selection, specify the options for executing the task as below:
    1. Check Disk: Select the drive that has to be checked and the required options and click Next. You can select from any of the following options:
        - *Verbose* - Displays the name of each file in every directory as the disk is checked.
        - *Quick Check* - This option is only available for NTFS file system. This skips the checking of cycles within the folder structure and performs a less vigorous check of index entries to reduce the time.
    2. Disk Cleanup: Select the files and folders to be cleaned and click Next. The following actions can be performed **
        - *Compress old files* - Windows can compress files that you have not used in a while. Compressing the files saves disk space while still enabling you to use them. No files are deleted. Because files are compressed at different rates, the displayed amount of disk space you will gain is approximate.
        - *Remove content indexer* - The Indexing service speeds up and improves file searches by maintaining an index of the files on the disk. These files are left over from a previous indexing operation and can be deleted safely.
        - *Remove downloaded Program Files* - Downloaded program files are ActiveX controls and Java programs that are downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.
        - *Remove internet cache files* - The Temporary Internet Files folder contains Web pages that are stored on your hard disk for quick viewing. Your personalized settings for Web pages are left intact.
        - *Remove Office setup files* - Installation files used by office. If these files are removed from your computer, you may be prompted for original installation media or source during Reinstall, Repair, or

Patch operation. It is recommended that you not remove these files unless you always have ready access to your installation media
- *Remove offline files* - Temporary files are local copies of network files that you specifically made available offline so that you can use them when you are disconnected from the network.
- *Remove old check disk files* - When Chkdsk checks your disk for errors, it might save lost file fragments as files in your disk's root folder. These files are unnecessary and can be removed.
- *Empty recycle bin* - The Recycle Bin contains files you have deleted from your computer. These files are not permanently removed until you empty the Recycle Bin.
- *Remove Temporary files* - Programs sometimes store temporary information in a Temp folder. Before a program quits, it usually deletes this information. You can safely delete temporary files that have not been modified in over a week.
- *Remove temporary offline files* - Temporary offline files are local copies of recently used network files that are automatically cached for you so that you can use them when you are disconnected from the network.
- *Remove Active Setup Temp Folders*
- *Remove memory dump files*
- *Remove remote desktop cache files*
- *Remove setup log files*
- *Remove old system restore positions.*
- *Remove web pages*
- *Remove uninstall backup images*
- *Remove webclient and web publisher cache files*

3. Disk Defragmenter: Select the drive that has to be defragmented and the required options and click Next. Seelct from the following options:
   - *Verbose*: Displays the complete analysis and defragmentation reports
   - *Analyze*: Analyzes the volume and displays a summary of the analysis report.
   - *Force Defragmentation*: Forces defragmentation of the drive regardless of whether it needs to be defragmented.

Step 2: Define Target

Using the Defining Targets procedure, define the targets for deploying the tasks.

Step 3: Define Scheduler

Specify the following scheduling options:

Parameter	Description
Run As*	The name of the user as whom the task will be run. Click the ☆ icon to select and assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.

Parameter	Description
Confirm Password	Confirm the password again.
Perform this task*	Specify the time to perform the task. You can select from the following options: • *Daily:* To run the task daily. Specify the time and duration to run the task. • *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. • *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. • *Once:* To run the task only once. You need to specify the date and time. • *At System Startup:* To run the task when the system is started. • *At Logon:* To run the task during the user logon. • *When Idle:* To run the task when the system is idle for the specified time.
Advanced Settings	
General	• *Enabled*: Select this option to run the task at the specified time. • *Run only when logged on:* Select this option to run the task only when the user has logged on.
Scheduled Task Completed	• *Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. • *Stop Task:* Select this option and specify the duration after which the task will be stopped.
Idle Time	Select the required options: • Specify the duration,the system has to be idle before starting a task. • Stop the task if the computer ceases to be idle
Power Management	Select the required options: • Don't start the task if the computer is running on batteries • Stop the task if battery mode begins • Wake the computer to run this task

Step 4: Deploy the Task

Click the **Deploy** button to deploy the task in the defined targets. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can

be verified from the Task Details page. Refer to the Viewing the Task History topic for details.

See Also: Viewing and Modifying the Tasks, Viewing Task History, Disk Defragmenter, Check Disk, Disk Cleanup

**The descriptions of various file types in Disk Cleanup are taken from Microsoft Help Documentation

Viewing and Modifying the Tasks

Viewing and Modifying the Tasks

Desktop Central allows creating multiple tasks that can be created to run various actions on different target computers at different intervals. You can view the tasks that are created by following the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled.
3. To modify a task,
    1. Click the icon from the Actions column of the corresponding task.
    2. This opens the Modify Configuration Wizard. You can add/remove tools, change the tool options, the target systems, and the scheduled time as required.
    3. Click **Deploy** to effect the changes.
4. To Delete a task, click the icon from the Actions column of the corresponding task.

See Also: Creating and Scheduling Tasks, Viewing Task History, Disk Defragmenter, Check Disk, Disk Cleanup

Viewing Task History


Viewing Task History

Desktop Central provides the details of the tasks executed on the target devices and the access logs of the tool execution.

Viewing Last Execution Status

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled.
3. Click on a task to view the details, such as the systems in which the task is executed, the last execution time, and the status of the task execution. Clicking the status will provide the access log of the performed task.

Viewing Task Execution History

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled.
3. To view the history of the task executed on a specific system, click the computer name. This will provide the history of the task execution on that computer along with the status on each execution. Clicking the status will provide the access log pertaining to that execution.

See Also: Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Disk Defragmenter, Check Disk, Disk Cleanup

Remote Desktop Sharing

Remote Desktop Sharing

Remote Desktop Sharing enables the administrators to gain access to remote Windows desktops in the network. It is a web-based tool enabling access from anywhere in the network without requiring any native client. It allows almost all operations to be performed on the remote desktop.

Remote Desktop Sharing – Advantages

1. No separate authentication is required to gain access to a remote desktop.
2. Supports viewing/accessing remote desktops using Active X and Java Plug-ins.
3. Prompts user confirmation before providing the access to a remote desktop.

Follow the links to learn more:

- Pre-requisites
- Connecting to Remote Desktop
- Troubleshooting Tips

Remote Desktop Sharing - Pre-requisites

Remote Desktop Sharing - Pre-requisites

To access remote desktops, the following pre-requisites have to be met:

1. Enable ActiveX Controls in the IE browser from where a connection is being established.
2. How to configure Firefox and Flock browsers for installing Desktop Central Add-on for Remote Desktop Sharing?
3. Installing Java Plug-ins in the Browser
4. Ports to be opened for Remote Control
5. Configuring Remote Desktop Settings

How to enable ActiveX Controls in Internet Explorer?

This configuration is required only in the browser from where a connection is being established

1. Select **Tools --> Internet Options** menu from the Internet Explorer.
2. Select the **Security** tab from the Internet Options dialog.
3. Select **Local Intranet** Web content zone and click **Custom Level**.
4. Make the following options available under ActiveX controls and plug-ins to either **Enable** or **Prompt**:
    1. Download signed ActiveX controls
    2. Download unsigned ActiveX controls
    3. Run ActiveX controls and plug-ins
    4. Script ActiveX controls marked safe for scripting
5. Click **OK** to save the Security Settings dialog.
6. Click **OK** to save and close the Internet Options dialog.

How to configure Firefox and Flock browsers for installing Desktop Central Add on for Remote Desktop Sharing?

This configuration is required only in the browser from where a connection is being established.

1. Select **Tools --> Options** menu from the browser.
2. Select the **Security** tab.
3. **Warn me when sites try to install add-ons** option will by default be enabled. Click the **Exceptions** button available beside it.
4. In the Allowed Sites dialog, add the name or the IP Address of the machine where Desktop Central Server is installed and click **Allow**.
5. Click **Close**.
6. Click **OK** to close the Options dialog.

When you try to access a remote desktop, you will be asked to install the Desktop Central Add on. Click Install to access the remote desktop.

Installing Java Plug-ins in the Browser

This configuration is required only in the browser from where a connection is being established and is required only when you choose the **Java Viewer** option when connecting to a remote desktop.

If Java plug-ins are already installed, the connection is automatically established. If not, you will be prompted to download and install Java Plug-in to connect to the remote desktop.

You can download the Java Plug-in can be downloaded from http://java.sun.com/products/plugin/ and install. You may have to restart the browser after installing the Java Plug-in.

Ports to be opened for Remote Control

Desktop Central requires TCP port **8443** to be opened in the machine where Desktop Central Server is installed. If you are running Windows Firewall, follow the steps below to add this port to the exceptions:

1. Select Start --> Settings --> Control Panel --> Windows Firewall
2. Select the Exceptions tab
3. Click Add Port button.
4. Specify a name.
5. Specify the Port as 8443.
6. Select the TCP option.
7. Click OK.

Configuring Remote Desktop Settings

Desktop Central supports prompting the user for confirmation before taking control of their desktop. This requires administrative privileges in Desktop Central. To enable or disable this option, follow the steps below:

1. Select **Tools --> Remote Control**
2. Select the option "**Prompt the User for Confirmation**" to take permission from the user before taking control of their desktop.
3. Click **Edit Settings** link to specify the following additional properties:
    1. Select the Viewer type as Active X or Java Viewer. This will be the default option chosen for the users and they can change as required.
    2. Select the option "Let users know that their desktop is shared" for the users to know that their desktop is being controlled by the administrator (even if the prompt is disabled).
    3. Select the option "Log the reason for remote connection" to make the users specify the reason for establishing connection to a remote computer.
    4. By default, the Remote Connection uses a secured communication at port 8443. If you wish to change the port specify the port number that has to be used in the port field. If you wish not to use a secured communication, clear the Use Secure Connection check box and specify the port number to be used. The port number that is specified here should be opened in the firewall of the computer where Desktop Central Server is installed.
    5. Select Enable Prompt option and specify the time to wait for user confirmation and the message to be displayed in the users' desktop. If the user do not confirm or decline within this time, the connection will not be established.

Connecting to Remote Desktop

Connecting to Remote Desktop

To connect to a remote desktop, follow the steps below:

1. Login to the Desktop Central client from an Internet Explorer or Firefox/Flock browsers. Ensure that the ActiveX Controls are enabled in the Internet Explorer or added Exceptions for installing Desktop Central Add-on in Firefox/Flock browsers.
2. Click the **Tools --> Remote Control**. This opens the Remote Control screen with the list of desktops available under the defined SoM.
3. You can also view the desktops that have the Desktop Central Agent installed, by selecting the "Show Agent Installed Computers" option. You can also filter the view based on the domains and remote offices.
4. Select the viewer as Active X or Java Viewer. For Java Viewer, you need to have java plug-ins installed in the browser.
5. Click **Connect** link under the Action column to connect to the desktop. You will see the status getting changed to connecting and subsequently to Connected. Now, click the **View Desktop** link to control the users' desktop.

	Note: When you are connecting to a remote desktop for the first time from a specific system, you must have logged in to the system with local administrative privileges. Subsequent connections from the same machine do not require this, as the necessary ActiveX controls and plug-ins would have got downloaded.

What can you do with this?

After establishing connection with a remote desktop, you can perform all actions that you would normally do from that system. For example, you can perform a configuration, start/stop applications, etc.

Once you have established connection with the remote desktop, you can use the toolbar to perform specific actions:

Toolbar Icon	Action
	To send ctrl+alt+del message to the remote computer
	Refreshes the view. If the computer is locked or no user has logged on, you will get the login dialog.
	To switch between different applications in the remote computer
	To black-out the users monitor so that the user may not see the actions performed in the remote computer.
	To lock the users keyboard and mouse.
	To unlock the users keyboard and mouse.
	Passes the control to you so that you can access it.
	Passes the control back to the user.
	Zooms in

Toolbar Icon	Action
	Zooms out
	Resets the view to its original size
	Resets the view size to fit to the screen
	Shows the remote desktop in full screen mode

Some of the known issues and limitation with respect to Remote Desktop Sharing has been listed here.

Auditing Remote Access Details

Whenever a user establishes a remote connection using Desktop Central, all the events performed on the remote computer are logged. Clicking the  icon available beside the computer name will list all the remote access made to that computer with the details of the user and the start/end time.

Troubleshooting Tips

Troubleshooting Tips

1. I was able to connect to a desktop from remote, but nothing is visible?
2. I am getting an "Access Denied" error when I try to connect to a remote desktop.
3. On connecting to a remote desktop, "The specified service does not exist as an installed service" error is shown.
4. When I select a desktop from the list, the status is always shown as not available, though the system is up.
5. I am getting an "The system cannot find the file specified" error when I try to connect to a remote desktop.
6. I was able to connect to a remote Desktop. But, the display is not proper.

1. I was able to connect to a desktop from remote, but nothing is visible?

Please check the following:

- Whether you have enabled ActiveX controls in the browser from where a connection is established. Refer to the Pre-requisites topic for details on configuration.
- If you are connecting to a desktop for the first time, log in to the system as a local administrator and connect. Subsequent connections from the same machine do not require administrative privileges as the necessary ActiveX controls and plug-ins would have got downloaded.

2. I am getting an "Access Denied" error when I try to connect to a remote desktop.

This error message is shown when the supplied credentials while defining the Scope of Management (SoM) is invalid or changed.

3. On connecting to a remote desktop, "The specified service does not exist as an installed service" error is shown.

This error message is shown when the Desktop Central Agent is not installed properly in the client machine. To reinstall the agent, follow the steps below:

1. Click the SoM link from the Quick Links.
2. Select the machines in which the agent needs to be re-installed and click **Install Agent**.

4. When I select a desktop from the list, the status is always shown as not available, though the system is up.

This happens when the client machine has firewall enabled with the "Don't Allow Exceptions" option selected. Disable the firewall to connect to that machine from remote.

5. I am getting an "The system cannot find the file specified" error when I try to connect to a remote desktop.

This error message is shown when one of the required files has been deleted from the client machine. Reinstall the agent as given below:

1. Click the SoM link from the Quick Links.
2. Select the machines in which the agent needs to be re-installed and click **Install Agent**.

6.I was able to connect to a remote Desktop. But, the display is not proper.

Try by changing the screen resolution using the Zoom in / Zoom Out icons.

Wake on LAN

- Creating and Scheduling Wake on LAN Tasks
- Viewing and Modifying Wake on LAN Tasks
- Viewing Wake on LAN Task Status
- Configuring Wake on LAN

The Wake on LAN Tool of Desktop Central helps to schedule booting of systems in the Windows Network remotely. It allows you to create different task to group the computers and specify a time to boot the machines in that task.

Creating and Scheduling Wake on LAN Tasks

To create a Wake on LAN task, follow the steps below:

Step 1: Define Task

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click the Wake on LAN tool listed under the Windows Tools category to open the task details page. This will list all the Wake on LAN tasks that have been created.
3. Click the Schedule Wake Up button to create a new task and specify the following:
    1. Provide a name of the task
    2. Choose the speed for the Wake on LAN task. Depending upon the selected speed, Desktop Central allocates more threads to complete the task.
    3. Waiting time after wake up: Specify the time in minutes after which the status gets updated in the Desktop Central client.
    4. Verify the computers already powered up before waking up: Select this option, if you wish to check the status before attempting to boot the machine.
    5. Use broadcast to wake up computers: Desktop Central supports sending both unicast and broadcast packets to boot the machines. When this option is not selected, Desktop Central first sends an unicast WOL packet to the machine to boot and check whether the machine is booted. If this fails, it broadcasts the WOL packet in the whole subnet.
    6. Resolve IP Address on each schedule: Select this option to resolve the IP Addresses of the machines during every schedule.

Step 2: Select Computers

1. Click Add Computers button to choose the computers for this task. The selected computers gets added to the table below.

2. Broadcasting of the WOL packtes is based on the subnet address of the computers. If the subnet address is blank of if it is incorrect, the task may fail. You can either click the icon and update the subnet address and MAC Address manually for individual computers ate select the computers in the same subnet and use the Set Subnet Address button to update the Subnet Address of multiple computers.

Step 3: Define Scheduler

1. *Once:* To run the task only once. You need to specify the date and time.
2. *Daily:* To run the task daily. Specify the time and duration to run the task.
3. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run.
4. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months.

Step 4: Deploy Task

Click the **Submit** button to deploy this task. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can be verified from the Task Details page.

Viewing and Modifying Wake on LAN Tasks

To view the Wake on LAN tasks that have been created, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click the Wake on LAN tool listed under the Windows Tools category to open the task details page. This lists all the tasks that are already created and scheduled.
3. To modify a task,
    1. Click the icon from the Actions column of the corresponding task.
    2. This opens the Modify task page. You can add/remove computers, change the task options, and the scheduled time as required.
    3. Click **Submit** to effect the changes.
4. To Delete a task, click the icon from the Actions column of the corresponding task.

Viewing Wake on LAN Task Status

To View the status of the Wake on LAN tasks that have ben created, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click the Wake on LAN tool listed under the Windows Tools category to open the task details page. This lists all the tasks that are already created and scheduled.
3. Click the Task name to view the status of the computers in that task.
4. You can filter to view the details of the computers by status like Scheduled, Processing, Success, and Failed.

Configuring Wake on LAN

BIOS Settings

The Wake-On-LAN functionality is generally disabled by default. The option to enable Wake-On-LAN is different with each computer manufacturer. The most common method adopted across different PC's are as follows:

1. During the computer's power-on self-test enter the BIOS setting screen by pressing the F1, INS, or DEL keys.
2. Select **Power** settings. Check for **Power Up Control**.
3. Enable settings related to Power Up on PCI card, LAN, or Network.
4. Click **Save** and exit the BIOS settings.

Operating System (OS) Settings

In some Windows OS, the drivers can enable the Wake ON LAN features of network adapters. For example in Windows 2000, click Power Management tab and under the **Adapters** properties, select the option **Allow this device to bring the computer out of standby**.

Alternatively, you can also check the **Advanced** setting table for parameters related to Wake on LAN and Waking on "Magic Packets" and enable them.

Wake-On-LAN (WOL) Cable

For Wake On LAN to work on computers with older PCI busses, a WOL cable must be installed between the Network Card and the Motherboard. Because this requires opening the computer case, we advice you to contact your PC manufacturer for specific instructions.

Enabling Directed Broadcasts on your Network

To send WOL packets from remote networks, the routers must be configured to allow directed broadcasts. To know if the IP broadcast packets have been disabled, check for the line "no ip directed-broadcast" in the interface configuration. If IP broadcasts are enabled, the line "no ip directed-broadcast" will not be present.

Remote Shutdown Tool

- Add Computers to Shutdown/Restart
- Shutdown Options
- Supported Operations
  - Shutdown
  - Restart
  - Hibernate
  - Stand by
  - Lock Computers
- Viewing the Status of the Operations
- Scheduling Shutdown
  - Creating and Scheduling Shutdown Tasks
  - Viewing and Modifying Shutdown Tasks
  - Viewing Shutdown Task Status

Remote Shutdown tool of Desktop Central provides options to shutdown, restart, lock, hibernate systems from remote, which is very useful for administrators.

Add Computers to Shutdown / Restart

Before adding computers to shutdown/restart, please ensure that you have specified a common credential to perform these actions in all the computers. To specify a credential, visit the Add Computers page.

To add computers to the list, follow the steps below:

1. Click the **Add Computers** button
2. Select a Domain/Workgroup to view the computers.
3. Select the computers to add and click **OK**.
4. The selected computers gets added to the table below.
5. Repeat steps two and three for adding computers from other domains/workgroups.

To remove computers from the list, select the computers and click **Remove Computers**.

Shutdown Options

When you try to shutdown or restart a computer, you need to specify the following options for shutting down:

- **Shutdown Mode**: This could be either of the following:
  - *Normal*: Select this option to close all the applications properly before shutting down the computer.
  - *Forced*: Select this option to terminate all the applications before shutting down the computers.
- **Timeout**: Specify the time in seconds to display a warning message in all the client computers before shutting down. Specify zero to skip the message and shutdown immediately.

- **Shutdown Message**: Specify the message to be displayed in all the computers before shutting down.

Supported Operations

You can perform the following operations on a remote computer:

- Shutdown
- Restart
- Hibernate
- Stand by
- Lock Computer

Shutdown

1. Add computers to the list
2. Select the computers from the list and click **Shutdown Now**
3. Specify the shutdown options and click **Shutdown**.
4. Click **Yes** to confirm

Restart

1. Add computers to the list
2. Select the computers from the list and click **Restart Now**
3. Specify the shutdown options and click **Restart**.
4. Click **Yes** to confirm

Hibernate

1. Add computers to the list
2. Select the computers from the list and select **Hibernate** from More Actions list.
3. Click **Yes** to confirm.

Stand by

1. Add computers to the list
2. Select the computers from the list and select **Stand by** from More Actions list.
3. Click **Yes** to confirm.

Lock Computers

1. Add computers to the list
2. Select the computers from the list and select **Lock Computers** from More Actions list.
3. Click **Yes** to confirm.

Viewing the Status of the Operation

The Remote Shutdown tool provides the following status values:

- **Last Operation** - denotes the last operation performed on a computer
- **Last Operation Initiated** - denotes the time at which the last operation was initiated
- **Status** - denotes the status of the last operation
- **Remarks** - to notify the details of errors encountered, if any.

Scheduling Shutdown

While it is possible to shutdown/restart/lock computers manually, it is also possible to schedule this to happen at periodic intervals.

- Creating and Scheduling Shutdown Tasks
- Viewing and Modifying Shutdown Tasks
- Viewing Shutdown Task Status

Creating and Scheduling Shutdown Tasks

To create a Shutdown task, follow the steps below:

Step 1: Define Task

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click the Remote Shutdown tool listed under the Windows Tools category. This opens the Remote Shutdown tool.
3. Select the Schedule Shutdown tab. This will list all the Shutdown tasks that have been created.
4. Click Add Shutdown Task and specify the following:
    1. Provide a name of the task
    2. Select the operation that has to be performed: Shutdown, Restart, Hibernate, Stand By, Lock Computer.
    3. When you select Shutdown or Restart options, you need to specify the Shutdown/Restart Options:
        1. **Shutdown Mode**: This could be either of the following:
            - *Normal*: Select this option to close all the applications properly before shutting down the computer.
            - *Forced*: Select this option to terminate all the applications before shutting down the computers.
            - **Timeout**: Specify the time in seconds to display a warning message in all the client computers before shutting down. Specify zero to skip the message and shutdown immediately.
            - **Shutdown Message**: Specify the message to be displayed in all the computers before shutting down.

Step 2: Add Computers

1. Click **Add Computers** button to choose the computers for this task.
2. The selected computers gets added to the table below.

Step 3: Configure Scheduler

1. *Once:* To run the task only once. You need to specify the date and time.
2. *Daily:* To run the task daily. Specify the time and duration to run the task.
3. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run.
4. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months.

Step 4: Deploy Task

1. Click the **Save Task** button to deploy this task. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can be verified from the Task Details page.

Viewing and Modifying Shutdown Tasks

To view the Shutdown tasks that have been created, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click the Remote Shutdown tool listed under the Windows Tools category. This opens the Remote Shutdown tool.
3. Select the Schedule Shutdown tab. This will list all the Shutdown tasks that have been created and scheduled.
4. To modify a task,
    1. Click the icon from the Actions column of the corresponding task.
    2. This opens the Modify task page. You can add/remove computers, change the task options, and the scheduled time as required.
    3. Click **Save Task** to effect the changes.
5. To Delete a task, click the icon from the Actions column of the corresponding task.

Viewing Shutdown Task Status

To View the status of the Shutdown tasks that have ben created, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click the Remote Shutdown tool listed under the Windows Tools category. This opens the Remote Shutdown tool.
3. Select the Schedule Shutdown tab. This will list all the Shutdown tasks that have been created and scheduled.
4. Click the Task name to view the status of the computers in that task.

Windows Configurations

Desktop Central enable remote configurations that can be applied to users and computers of the Windows domain-based network. The following sections guides you in configuring various Windows applications, security settings, display settings, firewall settings, and so on, to the Windows users and computers:

- User Configurations: Explains the various configurations that can be deployed to users using Desktop Central and the steps to define them.
- Computer Configurations: Explains the various configurations that can be deployed to computers using Desktop Central and the steps to define them.
- Configuring Collections: Helps you to define a collection configurations that can be deployed simultaneously for several users or computers.
- Defining Targets: Provides you the details of defining target computers and users for deploying the configuration.
- Managing Configurations and Collections: Helps you to manage the defined configurations, such as viewing the status of the defined configurations or collections, suspending the deployment, resuming the suspended deployments, and so on.
- Viewing Configuration Reports: Detailed report on the defined and deployed configurations using Desktop Central along with its status.
- Viewing System Uptime Reports: Provides the details of uptime and downtime of computers in the specified period.

How the Configurations gets Applied

Whenever a configuration is deployed using Desktop Central, it will be made available to the Desktop Central agents to apply the configurations in the client computers. The Desktop Central Agents residing at the client computers will pull the configuration details from the Server and process them. The Desktop Central agents will contact the Server at the following intervals to pull the details:

1. For user-specific configurations - during user logon and every 90 minutes thereafter till the user logs out of the domain.
2. For computer-specific configurations - during system startup and every 90 minutes thereafter till the system is shutdown.

User Configurations

User Configurations

This section details the configurations that can be applied to the users of the Windows Domain. These configurations are applied to the users during user logon or logoff.

	Note: Ensure that you have defined the scope of management before defining the configurations. For details, refer to Defining the Scope of Management.

To reach the configuration screen, follow the steps below:

1. Click **Add Configuration** link from the Quick Links. This will list all the supported configurations for users and computers.
2. Click the required configuration listed under the User Configurations.

Desktop Central supports the following configurations that can be applied on users:

- Configuring Alerts
- Executing Custom Scrips
- Configuring Display Settings
- Mapping Network Drives
- Setting Environment Variables
- Managing Files and Folders
- Redirecting User-Specific Folders
- Configuring Internet Explorer Settings
- Configuring IP Printer
- Launching Applications
- Displaying Message Box
- Configuring MS Office Settings
- Configuring Outlook Settings
- Setting Path
- Managing Permissions
- Configuring Power Options
- Configuring Registry Settings
- Securing USB Devices
- Configuring Security Policies
- Configuring Shared Printer
- Managing Shortcuts
- Installing Software - MSI/EXE Format

Configuring Alerts

Configuring Alerts

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Alert Configuration enables you to warn the users about the password expiration, lower hard disk space, and larger temp file size. The alert configuration are user-specific and requires the user to be logged on to view the alerts.

Step 1: Name the Configuration

Provide a name and description for the Alert Configuration.

Step 2: Define Configuration

The table given below lists the parameters for which alerts can be configured:

Parameter	Description
Password Expiration	The number of days before which the user has to be informed about the password expiration. The default value is 14 days.
Disk Space	The disk space in MB. When the disk space goes below the specified value the user will be warned.
Purge Temp Files	Specify whether to delete the temp files when exceeding the specified limit. You also have an option to specify the file types, size of the files, and whether to prompt the user before deleting the temp files or not.

Note: The alerts will be displayed during every logon of the user as long as the alert condition is met. For example, the user will be warned about the lower disk space during every logon until the free disk space exceeds the specified value.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Alert Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Alert Configuration in the targets defined. The alerts will be displayed when the defined conditions are met.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Executing Custom Scripts

Executing Custom Scripts

---

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Desktop Central provides options for configuring almost all the user configurations from remote. In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the user machines for accomplishing specific configurations. The scripts could be any of the following:

- Batch file (.bat or .cmd)
- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

Note: The script engines for languages like Perl, REXX, and Python, must be registered with Windows.

Step 1: Name the Configuration

Provide a name and description for the custom script configuration.

Step 2: Define Configuration

The table given below lists the parameters that have to be provided for defining the configuration.

Parameter	Description
Script Name*	The script that has to be executed in the user machines. You have an option to select the script from any of the following: • **Local**: The machine from where the configuration is being defined. • **Inventory**: Refers to the Desktop Central inventory. All the scripts that have been added using Managing Scripts procedure will be available here. • **Network Share**: Refers to the network share.
Script Arguments	The arguments that have to be provided while executing the scripts.
Execute During*	Refers to the script execution time. This can be either during the user **logon** or **logoff**.

* - Refers to the mandatory fields.

Note: The scripts specified from the **local** or **share**, will automatically be added to the Desktop Central inventory after successful deployment.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Custom Script Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Custom Script Configuration in the targets defined.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Managing Custom Scripts, Viewing Configuration Reports, Defining Targets

Configuring Display Settings

Configuring Display Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Display Configuration is for configuring the settings of Microsoft Windows Desktop such as welcome message, IntelliMouse tips, icons, folders and shortcuts, wallpaper, etc.

Step 1: Name the Configuration

Provide a name and description for the configuration.

Step 2: Define Configuration

The table below lists the display settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Wall Paper File	The wallpaper file (image file) that has to set as the desktop background. The wallpaper can be set from either local computer or from a network share by selecting the appropriate option. For wall papers that are set locally all the target computers should have the file in the same location. When choosing a file from network share, you can click the ☆ icon to select and assign a dynamic variable to this parameter.
Rename "My Computer" Icon	The name you wish to configure in place of "My Computer". Click the ☆ icon to select and assign a dynamic variable to this parameter.
Rename "My Network Places" Icon	The name you wish to have in place of "My Network Places". Click the ☆ icon to select and assign a dynamic variable to this parameter.
Remove "Windows Welcome Screen"	Select this option if you wish to remove the welcome message displayed by Windows.
Remove "Intellimouse Tips Screen"	Select this option to remove the intellimouse tips.
Remove "My Documents" Desktop Icon	Select this option to remove the "My Documents" icon from the desktop.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Display Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Display Configuration in the targets defined.

The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Mapping Network Drives

Mapping Network Drives

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Drive Mapping configuration enables you to map a remote network resource to the user machines. The mapped resource can then be accessed from the local machine using the drive name.

Step 1: Name the Configuration

Provide a name and description for the Drive Mapping configuration.

Step 2: Define Configuration

The table given below list the parameters that have to be specified for mapping a network drive:

Parameter	Description
Drive Name	The drive letter that has to be mapped with the resource.
Resource to be Shared	The shared resource in the network that has to be mapped.
Hide from Windows Explorer	To specify whether the mapping has to be hidden in the Windows Explorer. Select this option, if you want to hide.
Drive Label	The label name for the mapped drive that has to displayed in Windows Explorer.
Disconnect all existing network drives before mapping new	Specify whether to disconnect all the existing mappings or not.

Note:

1. To map more network drives, click **Add More Drives** and repeat Step 2. The mapped drive gets added to the **List of Drives to be Mapped** table.
2. To modify a mapping from this table, select the appropriate row, click icon and change the required values.
3. To delete a mapping from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Drive Mapping Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Drive Mapping Configuration in the targets defined. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Setting Environment Variables

Setting Environment Variables

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Environment variables are strings that contain information about the environment for the system, and the currently logged on user. Some software programs use the information to determine where to place files (such as temp, tmp, path etc). Environment variables control the behavior of various programs. Any user can add, modify, or remove a user environment variable. However, only an administrator can add, modify, or remove a system environment variable. Using Desktop Central, the environment variables can be defined and added.

Step 1: Name the Configuration

Provide a name and description for the Environment Variable configuration.

Step 2: Define Configuration

The following table lists the parameters that have to be specified**:**

Parameter	Description
Variable*	The environment variable name that has to be modified or added.
Value*	The value that has to be stored in the environment variable. Click the ☆ icon to select and assign a dynamic variable to this parameter.

* - denotes mandatory fields

Note:

1. To add more environment variables, click **Add More Variable** and repeat Step 2. The defined environment variable gets added to the **List of Environment Variable** table.
2. To modify a environment variable from this table, select the appropriate row, click icon and change the required values.
3. To delete a environment variable from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Environment Variable Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Environment Variable Configuration in the targets defined. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Path

Managing Files and Folders

Managing Files and Folders

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The File and Folder Operation allows you to copy, move, rename, delete files and folders of the users. Desktop Central File and Folder Operation Configuration enables you to copy/move/delete files for several users from central location.

Step 1: Name the Configuration

Provide a name and description for the File and Folder Operation configuration.

Step 2: Define Configuration

You can perform the following actions:

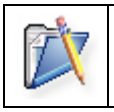
- Copy Files and Folders
- Rename/Move Files and Folders
- Delete Files and Folders

Copy Files and Folder

To copy files and folders, select the *Copy* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: • *Copy a File* - To copy a file from one location to another • *Copy a File to a Folder* - To copy a file from one location to a specified folder • *Copy Multiple Files* - To copy multiple files to a specified folder • *Copy a Folder* - To copy a folder from one location to another
Source File	Specify the file that has to be copied. The file can either be in a shared location or in the specified location in the client machines.
Destination File	Specify the destination location with the file name.

Parameter	Description
Destination Folder	Specify the destination folder to copy the files/folders.
Include Read Only Files	Select this option, if you wish to copy the files even if it has only read-only permissions
Include System Files	Select this option if you wish to copy the system files.
Include Hidden Files	Select this option if you wish to copy the hidden files.
Overwrite Existing Files	Select this option to overwrite the existing files.
Create Destination Directory if doesn't Exist	Select this option to create the destination directory, if it does not exist.
Include Sub Folders	Select this option, if you wish to copy sub folders or the files within the sub folders.
Continue on Error	While copying multiple files or folders, specify whether to continue, if any error is encountered while copying.
Choose file modification time	Specify the file or folder modification time. Files that meet the specified criteria will only be copied.



Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Rename / Move Files and Folders

To rename or move the files and folders, select the *Rename/Move* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: • Rename/Move a file • Rename/Move a folder
Source File/Folder	Specify the file or the folder that has to be copied
Destination File/Folder	Specify the destination file or the folder.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Delete Files and Folders

To delete the files and folders, select the *Delete* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: • Delete a File • Delete Multiple Files

Parameter	Description
	• Delete a Folder
Source File	Specify the files/folders that has to be deleted
Include Read Only Files	Select this option, if you wish to delete the read-only files
Include System Files	Select this option, if you wish to delete the system files
Include Hidden Files	Select this option, if you wish to delete the hidden files.
Include Sub Folders	Select this option, if you wish to delete the sub folders or the files within the sub folders.
Continue on Error	While deleting multiple files or folders, specify whether to continue, if any error is encountered while deleting.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

To modify a file action from the **List of File Actions** table, select the appropriate row and click icon and change the required values.

To delete a file action from the **List of File Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the File and Folder Operation Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined File and Folder Operation Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Redirecting User-Specific Folders

Redirecting User-Specific Folders

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Folder Redirection configuration helps you to change the location of the standard user profile directories to a different location in the network. So, when the user login from a different machine in the same domain, he/she will have access to his/her profiles.

Step 1: Name the Configuration

Provide a name and description for the Folder Redirection configuration.

Step 2: Define Configuration

You can perform the following actions:

- **Redirect the folders and copy the existing contents** - This redirects the user-specific folders from the local machine to a network share and copy the existing contents to the new location. You also have an option to exclude specific folders from being copied.
- **Redirect the folders without copying the contents** - This redirects the user-specific folders from the local machine to a network share without copying the existing contents.
- **Restore to default** - Will restore the settings to default (All folders will be pointed to the local machine).

Select the required options and specify the values for the following fields that require change in settings. For each of the fields in the following table, click the **Browse** button next to the corresponding field to launch **Network Browser** window. Select the folder location and click **OK** button. If this field is left blank, the corresponding folder settings is left unchanged.

The following table provides a brief description about the user-specific folders that can be redirected using Desktop Central.

User-specific Folder	Description
Start Menu*	Contains the shortcuts that appear in the start menu.
Programs Menu*	Contains the shortcuts that appear in the Programs group of the start menu.
Startup Group*	Contains the shortcuts that appear in Start --> Programs --> Startup menu. This specifies the applications that should be started during the user logon.

User-specific Folder	Description
Desktop*	Contains the shortcuts and files that appear in the user's desktop.
Favorites [IE Bookmarks]*	Contains the Internet Explorer bookmarks.
Personal [My Documents]*	Contains the personal documents of that user.
My Pictures*	Contains the personal pictures and images of that user.
Cookies*	Contains the cookies used by the Web sites/applications.
History*	Contains the bookmarks of the previously accessed sites.
Recent*	Contains the shortcuts of the recently accessed documents.
Temporary Internet Files*	The temporary Internet files are cached by Internet Explorer in this folder.
Send To*	Contains the shortcuts listed in the **Send To** sub-menu. The **Send To** sub-menu is displayed in the right-click menu of a file.
Exclude Folders	This option is available only when you choose to copy the existing contents. Specify the folders as comma separated that should not be copied.
Don't copy temporary internet files	This option is available only when you choose to copy the existing contents. Select this option if you do not wish to copy the temporary internet files.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Folder Redirection configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Folder Redirection Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Redirecting Common Folders

Installing Software - MSI & EXE Packages

Installing Software - MSI & EXE Packages

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Software Installation configuration helps you to install MSI and EXE packages remotely to specific users of several computers of the Windows network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Software Installation Configuration.

Step 2: Define Configuration

You have an option to install either an EXE or an MSI package

- Install MSI Package
- Install EXE Package

Install MSI Package

Select the Installer type as **MSI** and specify the following values:

Parameter	Description
MSI Package Name	This will list all the MSI packages that are available in the Software Repository. Select the MSI that has to be installed.
Run As	The user as whom the MSI has to be installed.
Password	Password for the user as whom the MSI has to be installed.
Confirm Password	Confirm the password
Operation Type	To specify how the installation should happen. Select any of the following options: • *Install Completely:* Selecting this option will install the application automatically during next GPO update or user logon or system startup. • *Assign*: Selecting this option will create all the necessary shortcuts and registry entries. The application will be installed only when the user tries to open the application or during system

Parameter	Description
	startup, whichever is earlier. • *Remove*: Selecting this option remove (uninstall) the application from the system • *Redeploy*: Selecting this option will re-install the application.
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: • *None:* Selecting this option will not copy the installation files. • *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. • *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after user login: • *During Login*: Select this option if the software has to be installed/uninstalled during the user login. • *After Login*: Select this option if the software has to be installed/uninstalled after the user login but within 90 minutes. • *During or After Login*: Either of the above, whichever is earlier
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type selected, but this will begin after the time specified here.
Reboot Policy	• *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. • *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. • *Force Shutdown when the user has logged in*:

Parameter	Description
	Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. • *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. • *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Install EXE Packages

Select the Installer type as **EXE** and specify the following values:

Parameter	Description
EXE Package Name	This will list all the EXE packages that are available in the Software Repository. Select the EXE that has to be installed.
Run As	The user as whom the EXE has to be installed.
Password	Password for the user as whom the EXE has to be installed.
Confirm Password	Confirm the password
Operation Type	To specify how the installation should happen. Select any of the following options: • *Install:* Selecting this option will install the application automatically during next GPO update or user logon or system startup. • *Remove*: Selecting this option remove (uninstall) the application from the system
Copy the Source File & Folder to client machines	Selecting this option will copy all the necessary installables to the client machines.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after user login: • *During Login*: Select this option if the software has to be installed/uninstalled during the user login.

Parameter	Description
	• *After Login*: Select this option if the software has to be installed/uninstalled after the user login but within 90 minutes. • *During or After Login*: Either of the above, whichever is earlier
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type selected, but this will begin after the time specified here.
Reboot Policy	• *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. • *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. • *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. • *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. • *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Windows Installer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Windows Installer Configuration in the defined targets. The software installation for the selected targets will happen as scheduled.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Internet Explorer Settings

Configuring Internet Explorer Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Internet Explorer settings such as Home page, Search page, Download directory, and Proxy Server settings can be configured using Desktop Central Internet Explorer Configuration.

Step 1: Name the Configuration

Provide a name and description for the Internet Explorer configuration.

Step 2 Define Configuration

The following table provides the Internet Explorer parameters that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Home Page	Refers to the page that opens when the Internet Explorer is started.
Search Page	Refers to the search engine that Internet Explorer uses when clicked on the Search button from the toolbar.
Download Directory	Refers to the location where the file downloads are redirected. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Automatic Configuration Script	Refers to the URL of the script that is used to configure the proxy settings of Internet Explorer.
Internet Connection Wizard	The Internet Connection Wizard is invoked when a user tries to launch the Internet Explorer for the first time. Specify whether to remove or retain this.
Proxy Server	A proxy server is a server that acts as an intermediate between the computer in the network and the Internet, and that ensures security, administrative control, and caching. Select the appropriate proxy setting.
Address**	The IP address or host name of the Proxy Server.
Port**	The port number of the Proxy Server
Bypass for local addresses**	Specifies how the request has to be routed when a local address is accessed using the Internet Explorer. Select any of the following options: • **Bypass proxy server:** Select this option if the

Parameter	Description
	request should not be routed through the proxy server for local addresses. • **Dont Bypass proxy server:** Select this option if the request should be routed through the proxy server even for local addresses. • **Preserve Client Settings:** To preserve the settings of the client untouched.
Do not use proxy server for addresses beginning with**	The list of addresses that begins with the text specified in this field will not use the Proxy Server. You can specify multiple values as semi-colon separated. Example: `adventnet.com;desktopcentral.com` This field is enabled only when Bypass Proxy server option is selected.

** - required only if **Use Proxy Server** option is selected.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Internet Explorer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Internet Explorer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring IP Printer

Configuring IP Printer

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The IP Printer Configuration is for adding or deleting the IP Printer connection in the user computers. For configuring a shared printer in the computer for specific users, refer to the Configuring Shared Printer topic.

Step 1: Name the Configuration

Provide a name and description for the IP Printer configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add an IP Printer
- Delete an IP Printer

Add an IP Printer

To add an IP Printer, select the **Action** as *Add* and specify the following values:

Parameter	Description
DNS Name/IP	The host name or IP address defined for the printer. *Example*: 192.111.2.32
Printer Name	The display name for the printer.
Protocol	The printing protocol supported by the printer. Select the printing protocol from the Protocol list box. The default option is "RAW".
Port Number	The port number/queue name in which printing protocol is communicating between the computer and printer. Enter the port number in the Port Number field if the "RAW" Protocol is selected or enter the queue name if the "LPR" Protocol is selected. The default value is 9100.
Port Name	This is an optional field. By default, the port name is IP_<IP_Address/DNS_Name>. You can change the port name if required.

Parameter	Description
Shared Printer for Driver Installation	Browse to select a shared printer for installing the driver. If the drivers are already installed in the target computers, this field can be left blank.
Set as default printer	To configure the configured IP Printer connection on the computer as the default printer in the computer for a specific user, select this option.

Delete an IP Printer

To delete an IP Printer, select the **Action** as *Delete* and specify the following values:

Parameter	Description
Printer Name	The display name of the printer.
Delete all existing IP printer connections	To delete all the existing IP printer connections in the computer for the specified user, select this option.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the IP Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined IP Printer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Configuring Shared Printer

Launching Applications

Launching Applications

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Launch Application configuration enables you to launch an application during user logon.

Step 1: Name the Configuration

Provide a name and description for the Launch Application configuration.

Step 2: Define Configuration

Select whether the application has to be launched from the local computer or from the network share. If you select the Local option, all the selected target computers should have the application in the same location. Specify the following:

Parameter	Description
Application Name	Browse and select the application that has to be launched. The applications that are available in the local machine from where the application has to be launched can also be specified. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Arguments	Specify the arguments for the application, if any. Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note:

1. To launch more applications, click **Add More Application** and repeat Step 2. The added application gets added to the **Launch Application** table.
2. To modify an application from this table, select the appropriate row, click icon and change the required values.
3. To delete an application from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Launch Application Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Launch Application Configuration in the targets defined. The applications configured will be launched during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Displaying Message Box

Displaying Message Box

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

For the users in the network, the pop-up messages with the warning or error can be displayed during the user logon. If the user has already logged on while deploying this configuration, the message will be displayed during the next logon.

Step 1: Name the Configuration

Provide a name and description for the Message Box configuration.

Step 2: Define Configuration

You have an option to create a new message box or delete the existing message box. Select the required option and specify the following:

Parameter	Description
Message Type	The message type as Information, Warning, or error.
Window Title	The title of the message box.
Message	The message that has to be displayed.
Timeout in Seconds	The duration, in seconds, for the message display.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Message Boxes Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Message Boxes Configuration in the targets defined. The message will be displayed during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Displaying Legal Notices

Configuring MS Office Settings

Configuring MS Office Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The MS Office related settings such as Open or Save, Clip Art, User Options, Command Bars, Shared Template, etc can be configured for all the users using Desktop Central MS Office Configuration.

Step 1: Name the Configuration

Provide a name and description for the MS Office configuration.

Step 2: Define Configuration

The MS Office applications that can be configured using Desktop Central are listed in the Choose Application/Suite combo box. Select the application version and specify the values that have to be changed. Leave it blank, if no change is required.

The following table lists the parameters that can be configured for each MS Office applications:

Parameter	Description
Word	
Open/Save Folder*	Refers to the default working folder for Microsoft Word. Clicking Open or Save menu will open this folder location.
Clip Art Folder*	Refers to the default Clip Art folder. This opens when you insert an image from the clip art.
User Options Folder*	Refers to the folder where the user options are stored.
Tools Folder*	Refers to the folder where the office tools are stored.
Auto Recover Folder*	Refers to the folder where the recovered files are stored due to the system crash.
Startup Folder*	Refers to the location where the templates and add-ins are loaded during the startup of Microsoft Word.
Excel	
Open/Save Folder*	Refers to the default working folder for Microsoft Excel. Clicking Open or Save menu will open this folder location.

Parameter	Description
At startup, open all files in*	Refers to the folder containing the files that have to be opened during startup.
Access	
Open/Save Folder*	Refers to the default working folder for Microsoft Access. Clicking Open or Save menu will open this folder location.
Command Bars Folder*	Refers to the location where the command bar buttons of Microsoft Access are stored.
PowerPoint	
Open/Save Folder*	Refers to the default working folder for Microsoft Powerpoint. Clicking Open or Save menu will open this folder location.
Command Bars Folder*	Refers to the location where the command bar buttons of Microsoft Powerpoint are stored.
Office	
Template Folder*	Refers to the location where the Microsoft Office templates are stored.
Shared Template Folder*	Refers to the location where the shared Microsoft Office templates are stored.
Outlook	
Journal Item Log File*	Refers to the location where the old journal item file is stored.
Journal Outlook Item Log File*	Refers to the location where the old journal item file that is referred by the journal entry is stored.
Office Explorer Favorites Folder*	Refers to the default location for storing the favorites. Clicking the Add Favorites menu item will store the URLs in this location.
Office Explorer Views Folder*	Refers to the location where the user views are stored.
Print Settings File*	Refers to the file which stores the print styles of the user views.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the MS Office Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined MS Office Configuration for the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Outlook Settings

Configuring Outlook Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Microsoft Outlook settings such as general settings, new mail arrival, automatic archive, sending a message, message format and handling, and spell check can be configured. The Outlook Configuration is used to configure these settings for the users of the network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Outlook configuration.

Step 2: Define Configuration

The table given below lists the Outlook parameters that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
General Settings	
View Outlook Bar	To show or hide the Outlook shortcut bar when Outlook is opened.
View Folder List	To show or hide the folders listed when Outlook is opened.
Warn before deleting items	To enable or disable the warning message when deleting entries from the *Deleted Items* folder.
Startup in this Folder	The folder which must be opened after the Outlook is invoked. Select from the following options: *Outlook Today*, *Inbox*, *Calendar*, *Contacts*, *Tasks*, *Journal*, *Notes*, and *User-defined*. Select *User-defined* option to make the user configure this option.
Empty the Deleted Items folder upon exit	Select the frequency at which the contents of the *Deleted Items* folder should be cleared when exiting the Outlook. Select *User-defined* option to make the user configure this option.
New mail arrival	
Display a New mail Desktop Alert	To enable or disable the notification message when a new mail arrives.
Play a sound	To enable or disable playing sound when a new mail arrives.

Parameter	Description
AutoArchive	
Run AutoArchive	To enable or disable the automatic archiving of folder. Specify the required option and choose the frequency at which archiving should be done.
Prompt to AutoArchive	To specify whether to prompt before archiving or not.
Move old items to	The location where the archived files must be stored. Click the ☆ icon to select and assign a dynamic variable to this parameter.
File name	The name of the archived file.
Delete expired items (e-mail folders only)	To specify whether the expired items should be deleted or not.
When sending a message	
Allow comma as address separator	To specify whether comma should be used as a address separator or not.
Automatic name checking	To enable or disable automatic checking for the validity of names in the recipient list.
Message format & handling	
Compose in this Message Format	Select the message format as *HTML*, *Rich Text*, or *Plain Text*. Select User-defined to leave it to the user to configure.
Use Microsoft Word to edit email messages	Specify whether Word should be used as a default editor.
Send a copy of the pictures instead of the reference to their location (only for HTML format)	To specify whether to send pictures along with the mail or not.
Save copies in Sent items folder	To specify whether to save copies in the sent folder or not.
Autosave unsent	To specify whether to save the unsent messages or not. Select the frequency if you are enabling this option.
Spelling	
Always check spelling before sending	To specify whether to check spelling before sending the message or not.
Always suggest replacements for misspelled words	To specify whether to suggest replacement for misspelt words or not.
Ignore words in UPPERCASE	To enable or disable checking words in upper case letters.
Ignore words with numbers	To enable or disable checking words containing numbers.
Ignore original message in replies	To enable or disable checking the spelling of original mails in replies.

Step 3: Define Target

Using the Defining targets procedure, define the targets for deploying the Outlook Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Outlook Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Setting Path

 **Setting Path**

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

For the users in the network, the paths which are configured and stored in the **Path** variable in the **Environment Variables** window (invoked by Right-click the **My Computer** icon, choose **Properties** > **Advanced** tab, click the **Environment Variables** button). The search paths including local paths, network paths or UNCs (Universal Naming Conventions). Using the Path Configuration, the path entries are added in the **Environment Variables** window for the users in the network.

Step 1: Name the Configuration

Provide a name and description for the Path configuration.

Step 2: Define Configuration

Specify the path to be added to the environment variables. Multiple paths can be specified separated by a semi-colon (**;**). Click the ☆ icon to select and assign a dynamic variable to the Path variable.

Step 3: Define Target

Using the Defining targets procedure, define the targets for deploying the Path Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Path Configuration in the defined targets. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Environment Variables

Managing Permissions

Managing Permissions

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Permission Management allows you to grant revoke permission on the files, folders and registry for the users. Desktop Central Permission Management Configuration enables you to grant/revoke permissions to multiple users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Permission Management configuration.

Step 2: Define Configuration

You can grant or revoke permissions for the following objects:

- Files
- Folders
- Registry

Files

To grant or revoke permissions for files, select the *File* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: • Append - To append to the existing file permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. • Overwrite - To overwrite the existing file permissions • Revoke - To revoke the existing file

Parameter	Description
	permissions of the specified user/group. All the permissions to the specified user/group on that file will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the file for which you need to specify permissions
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Folders

To grant or revoke permissions for folders, select the *Folder* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: • Append - To append to the existing folder permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. • Overwrite - To overwrite the existing folder permissions • Revoke - To revoke the existing folder permissions. All the permissions to the specified user/group on that folder will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the folder for which you need to specify permissions
Inheritance	Select the required option to specify how the permission should effect its subfolders and files
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Registry

To grant or revoke permissions for registry, select the *Registry* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: • Append - To append to the existing registry permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. • Overwrite - To overwrite the existing registry permissions • Revoke - To revoke the existing registry permissions. All the permissions to the specified user/group on that registry key will be removed. However, the inherited permissions will not be removed.
Hive	Select the registry hive from the given options
Key	Specify the key within that hive for which you need to set the permissions
Inheritance	Select the required options to specify how the permission should effect its subkeys.
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

To modify a permission from the **List of Permission Actions** table, select the appropriate row and click icon and change the required values.

To delete a permission from the **List of Permission Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Permission Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Permission Management Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Power Options

Configuring Power Options

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Power Management Configuration enables you to adjust your power settings to save energy. You can add, modify, and delete power schemes for users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Power Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Power Scheme
- Delete a Power Scheme

Create / Modify a Power Scheme

To create a new scheme, select the **Create Scheme** tab of the Power Management Configuration. Select the **Modify Scheme** tab to modify an existing scheme. Specify the following values:

Parameter	Description
Power Scheme*	The name of the power scheme that has to be created/modified. If you are modifying a default scheme, select the Default Scheme option and select the scheme.
Overwrite if scheme already exits	Select this option to overwrite the scheme, if one with the same name exists. This option is only available for create scheme.
Set as active power scheme	Select this option if you wish to make this scheme active. Clearing this option will only create or modify the scheme and the system will continue to use the previously applied scheme.
Turn Off Monitor	Turns off the monitor after the specified period of inactivity. Select the period from the combo box.
Turn Off Hard Disk	Turns off the hard disk after the specified period of inactivity. Select the period from the combo box.

Parameter	Description
System StandBy	The system goes to the standby mode after the specified period of inactivity. Select the period from the combo box.
System Hibernate	Turns off the computer after saving everything in memory to the hard disk after the specified period of inactivity. When the system is turned on again, it is restored to the same position. Select the period from the combo box.
Advanced Options	
Enable Hibernate support	Select this option to enable hibernation of the computer.
Always show icon on the taskbar	Select this option to display the power icon in the system tray.
Prompt for password when computer goes off StandBy	Select this option, if you wish the user to authenticate himself/herself when the computer is resumed from standby mode.
When I close lid	Select the action to be performed on closing the lid. It can be either left as such or made to go to the standby mode.
When I press the power button on my computer	Select the action to be performed when the power button is pressed from the following options: • Do nothing - to leave it as such • Ask me what to do - to prompt the user • Standby - to go to the standby mode • Shutdown to shutdown the computer
When I press the sleep button on my computer	Select the action to be performed when the sleep button is pressed from the following options: • Do nothing - to leave it as such • Ask me what to do - to prompt the user • Standby - to go to the standby mode • Shutdown to shutdown the computer

* - denotes mandatory parameters

Note: While creating new schemes, you can select any of the default schemes from the list to load its values and then modify it to suit your need.

If you wish to create/modify more schemes, click **Add More Scheme** button and repeat step 2. The defined scheme gets added to the **List of Power Schemes added** table.

Delete a Power Scheme

To delete an existing power scheme, select the Delete Scheme tab of the Power Management Configuration and specify the name of the scheme that has to be deleted.

If you wish to create/modify/delete more schemes, click **Add More Scheme** button and repeat step 2. The defined task gets added to the **List of Power Schemes added** table.

To modify a scheme from **List of Power Schemes added** table, select the appropriate row and click icon and change the required values.

To delete scheme from **List of Power Schemes added** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Power Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Power Management Configuration in the defined targets. The Power Management configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Registry Settings

Configuring Registry Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Registry Settings allows you to add, modify, and delete the values in the registry of the users. Desktop Central Registry Settings Configuration enables you to modify the values in the registry centrally and for several users.

Step 1: Name the Configuration

Provide a name and description for the Registry Settings configuration.

Step 2: Define Configuration

You can perform the following actions:

- Write Value
- Delete Value
- Add Key
- Delete Key

Write Value

To write a value in the registry, select the **Action** as *Write Value* and specify the following values:

Parameter	Description
Header Key	Select the header key from the following options: • *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. • *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. • *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. • *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value.

Parameter	Description
Type	The type of the value. This varies with respect to the Header Key selected. Select the appropriate type from the combo box.
Value	Specify the value to be added. Click the icon to select and assign a dynamic variable to this parameter.
Data / Expression	Specify the data or expression. If the new value has to be created without data, enter the word clear inside the parentheses as (clear). Click the icon to select and assign a dynamic variable to this parameter.

Note: If you wish to write more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Value

To delete a value from the registry, select the **Action** as *Delete Value* and specify the following values:

Parameter	Description
Header Key	Select the header key from the following options: • *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. • *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. • *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. • *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value.
Value	Specify the value to be deleted.

Note: If you wish to delete more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Add Key

To add a registry key, select the **Action** as *Add Key* and specify the following:

Parameter	Description
Header Key	Select the header key from the following options: • *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. • *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. • *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. • *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value to be added.

Note: If you wish to add more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Key

To delete a registry key, select the **Action** as *Delete Key* and specify the following values:

Parameter	Description
Header Key	Select the header key from the following options: • *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. • *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. • *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. • *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value that has to be deleted.

Note: If you wish to delete more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

To modify a registry setting from the **Registry Settings** table, select the appropriate row and click icon and change the required values.

To delete a registry setting from the **Registry Settings** table, select the appropriate row and click  icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Registry Settings Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Registry Settings Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Securing USB Devices

Securing USB Devices

---

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Secure USB Configuration is used to Enable or Disable the selected USB Devices for individual users. This configuration will be applicable to a particular user irrespective of the computer he uses to log on.

Step 1: Name the Configuration

Provide a name and description for the Secure USB configuration.

Step 2: Define Configuration

1. **Select the devices to be enabled / disabled from the given list:**
    - Mouse
    - Disk Drive
    - CD-ROM
    - Portable Devices
    - Floppy Disk
    - Bluetooth
    - Image
    - Printer
    - Modem
2. **LogOff Action**

    The LogOff Action setting helps you to retain/revoke the Secure USB configuration when the User Logs Off.

    - Don't Alter Device status - Select this option to retain the configurations
    - Disable All Devices Excluding Mouse - Select this option to revoke all the Secure USB configuration of the user when he logs-off.

Note: It is desirable to define and deploy Secure USB configurations at the computer-level. This is required because, all the user-specific USB configurations are also set at the computer level. The sequence of operations during system startup and user logon/logoff given below helps you to understand better:

- System Startup - The Secure USB configuration defined at the computer-level gets applied.
- User logon - The Secure USB configuration defined at the computer-level gets applied first. Then, Secure USB configuration defined for that user, if any, gets over-written.
- User Logoff - The Logoff action defined for that user gets applied.

From the above, if there is no computer configuration has been defined for securing the USB drives and if the LogOff Action is set at "Don't Alter Device Status", the user configuration will be available for other users who log on to that computer subsequently who do not have any specific configurations defined for them.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Secure USB Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Secure USB Configuration in the targets defined. The configuration will take effect during the next user logon.
To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Securing USB for Computers

Configuring Security Policies

Configuring Security Policies

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Security policies determine the various security restrictions that can be imposed on the users in a network. The security settings for Active Desktop, Computer, Control Panel, Explorer, Internet Explorer, Network, and System categories can be defined using **Security Policies Configuration**.

Step 1: Name the Configuration

Provide a name and description for the Security Policies Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Choose Policy Category	The specific policy area in which the security policy will be applied. Select the desired category from left. This displays the relevant security polices. For details on the each category, refer to Windows Help documentation. For details on the each policy in the **Select the Policy** list, refer to Security Policies topic.
Policy Value	To enable, disable, or to leave it unconfigured, select the appropriate option.

Note:
1. To modify a security policy from this table, select the appropriate row, click icon and change the required values.
2. To delete a security policy from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Security Policies Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Security Policies Configuration in the defined targets. The security policies will be applied during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Security Policies

Configuring Shared Printer

Configuring Shared Printer

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

When a printer is installed in a machine in the network and is shared, other machines in the network can use this printer for their printing needs. Desktop Central enables you to configure the shared printer in the user machines.

For configuring an IP printer connection to the computer, refer to the Configuring IP Printer topic.

Note: To add the Shared Printer Configuration, a computer must be installed with printer connection and must be shared.

Step 1: Name the Configuration

Provide a name and description for the Shared Printer Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add a Shared Printer
- Delete a Shared Printer

Add a Shared Printer

To add a shared printer, select the **Action** as *Add* and specify the following values:

Parameter	Description
Shared Printer Path*	Browse and select the path of the shared printer location in the network.
Set as default printer	Select this check box, if you want to make this as the default printer for the user. By default, this option is cleared.

* - denotes mandatory field

Delete a Shared Printer

To delete a shared printer, select the **Action** as *Delete* and specify the following values:

Parameter	Description
Shared Printer Path*	Browse and select the path of the shared printer location in the network.
Delete all existing network shared printer connections	Select this check box, if you want to delete all the existing shared printer connections. By default, this option is disabled.

* - denotes mandatory field

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shared Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shared Printer Configuration in the defined targets. The printer configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Managing Shortcuts

Managing Shortcuts

---

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The shortcut is an icon that points to a file or folder. The Shortcut Configuration enables you to add shortcuts to the users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Shortcut Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create a Shortcut
- Delete a Shortcut

Create a Shortcut

To create a shortcut, select the **Action** as *Create Shortcut* and specify the following values:

Parameter	Description
Overwrite	To modify the existing shortcut select this option.
Shortcut Name*	Specify the name of the shortcut.
Target Application*	Browse and select the target application from the network for which a shortcut has to be created. The target application can also be in the local machine where the configuration is being deployed.
Arguments*	If the application requires any arguments, specify the arguments. Leave it blank if it does not require any arguments.
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: • *User Desktop*: Refers to the desktop of that user.

Parameter	Description
	• *User Favorites*: Refers to the favorites folder of that user. • *User Start Menu*: Refers to the start menu of that user. • *User Programs Group*: Refers to the Start --> Programs group of that user. • *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. • *User Quick Launch Bar*: Refers to the quick launch bar of that user. • *All Users Desktop*: Refers to the desktop common for all the users. • *All Users Start Menu*: Refers to the start menu common for all users. • *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. • *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Start In Folder*	Some applications may have some references to additional files during execution. In such cases, browse and select the location from where the application has to be started.
Shortcut Comments	Specify the comments for this shortcut.
Icon File*	Browse and select the icon for the shortcut.
Run Window	Select how the application has be started - *Normal*, *Maximized*, or *Minimized*.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to create more shortcuts, click **Add Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

Delete a Shortcut

To delete a shortcut, select the **Action** as *Delete Shortcut* and specify the following values:

Parameter	Description
Shortcut Name	Specify the name of the shortcut. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Shortcut Location	Select the location from where the shourcuts needs to be deleted. The shortcut location can be any of the following: • *User Desktop*: Refers to the desktop

Parameter	Description
	of that user. • *User Favorites*: Refers to the favorites folder of that user. • *User Start Menu*: Refers to the start menu of that user. • *User Programs Group*: Refers to the Start --> Programs group of that user. • *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. • *User Quick Launch Bar*: Refers to the quick launch bar of that user. • *All Users Desktop*: Refers to the desktop common for all the users. • *All Users Start Menu*: Refers to the start menu common for all users. • *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. • *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

Note: If you wish to delete more shortcuts, click **Add More Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

To modify a shortcut from the **Shortcut** table, select the appropriate row and click icon and change the required values.

To delete a shortcut from the **Shortcut** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shortcut Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shortcut Configuration in the defined targets. The shortcut configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Computer Configurations

Computer Configurations

This section details the configurations that can be applied to the computers of the Windows Domain. Configurations applied to computers are available for all the users of the computers. These configurations are applied to the computers during startup or shutdown.

	Note: Ensure that you have defined the scope of management before defining the configurations. For details, refer to Defining the Scope of Management.

To reach the configuration screen, follow the steps below:

1. Click **Add Configuration** link from the Quick Links. This will list all the supported configurations for users and computers.
2. Click the required configuration listed under the Computer Configurations.

Desktop Central supports the following configurations that can be applied on computers:

- Redirecting Common Folders
- Executing Custom Scripts
- Setting Environment Variables
- Managing Files and Folders
- Configuring Windows XP Firewall
- Configuring General Computer Settings
- Managing Windows Local Groups
- Installing Patches
- Installing Software - MSI/EXE Format
- Installing Windows Service Packs
- Configuring IP Printers
- Launching Applications
- Displaying Legal Notices
- Displaying Message Box
- Setting Path
- Managing Permissions
- Configuring Registry Settings
- Securing USB Devices
- Scheduling Tasks
- Configuring Security Policies
- Managing Shortcuts
- Configuring Windows Services
- Managing Windows Local Users

Redirecting Common Folders

Redirecting Common Folders

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Common Folder Redirection Configuration helps to change the location of the All User Shell folders that are shared by all the users. The All User Shell folders which contains common Start Menu, Programs Group, Startup Group, Desktop, and application data shared by all the users. For the redirection of the user-specific folders in the computer, refer to the Redirecting User-Specific Folders topic.

Step 1: Name the Configuration

Provide a name and description for the Common Folder Redirection Configuration.

Step 2: Define Configuration

Select the values for the following fields that require change in settings. For each of the fields in the following table, click the **Browse** button next to the corresponding field to launch **Network Browser** window. Select the folder location and click **OK** button. If this field is left blank, the corresponding folder settings is left unchanged.

The following table provides a brief description about the common folders that can be redirected using Desktop Central.

Field	Description
Common Start Menu*	Contains the shortcuts that appear in the start menu that are common for all the users of the computer.
Common Programs Group*	Contains the shortcuts that appear in the Programs group of the start menu that are common for all the users of the computer.
Common Startup Group*	Contains the shortcuts that appear in Start --> Programs --> Startup menu. This specifies the applications that should be started during the startup of the system.
Common Desktop*	Contains the shortcuts and files that appear in the desktop that are common for all the users of the computer.
Common Application Data*	Contains the application data that are shared by all the users (C:/Documents and Settings/All Users/Application Data).

* - Click the icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Common Folder Redirection Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Common Folder Redirection Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Redirecting User-Specific Folders

Executing Custom Scripts

Executing Custom Scripts

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Desktop Central provides options for configuring almost all the computer configurations from remote. In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the machines for accomplishing specific configurations. The scripts could be any of the following:

- Batch file (.bat or .cmd)
- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

Note: The script engines for languages like Perl, REXX, and Python, must be registered with Windows.

Step 1: Name the Configuration

Provide a name and description for the Custom Script Configuration.

Step 2: Define Configuration

The table given below lists the parameters that have to be provided for defining the configuration.

Parameter	Description
Script Name*	The script that has to be executed in the machines. You have an option to select the script from any of the following: • **Local**: The machine from where the configuration is being defined. • **Inventory**: Refers to the Desktop Central inventory. All the scripts that have been added using Managing Scripts procedure will be available here. • **Network Share**: Refers to the network share.
Script Arguments	The arguments that have to be provided while executing the scripts.
Execute During*	Refers to the script execution time. This can be either during the system **startup** or **shutdown**.

* - Refers to the mandatory fields.

Note: The scripts specified from the **local** or **share**, will automatically be added to the Desktop Central inventory after successful deployment.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Custom Script Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Custom Script Configuration in the targets.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Managing Custom Scripts

Setting Environment Variables

Setting Environment Variables

1. Name the Configuration
2. Defining Configuration
3. Defining Target
4. Deploy Configuration

Environment variables are strings that contain information about the environment for the system, and the currently logged on user. Some software programs use the information to determine where to place files (such as temp, tmp, path etc). Environment variables control the behavior of various programs. Any user can add, modify, or remove a user environment variable. However, only an administrator can add, modify, or remove a system environment variable. Using Desktop Central, the environment variables can be defined and added.

Step 1: Name the Configuration

Provide a name and description for the Environment Variable Configuration.

Step 2: Define Configuration

The following table lists the parameters that have to be specified**:**

Parameter	Description
Variable*	The environment variable name that has to be modified or added.
Value*	The value that has to be stored in the environment variable. Click the icon to select and assign a dynamic variable to this parameter.

* - denotes mandatory fields

Note:
1. To add more environment variables, click **Add More Variables** and repeat Step 2. The defined environment variable gets added to the **List of Environment Variable** table.
2. To modify a environment variable from this table, select the appropriate row, click icon and change the required values.
3. To delete a environment variable from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Environment Variable Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Environment Variable Configuration in the targets defined. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Path

Managing Files and Folders

Managing Files and Folders

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The File and Folder Operation allows you to copy, move, rename, delete files and folders in computers. Desktop Central File and Folder Operation Configuration enables you to copy/move/delete files for several computers from central location.

Step 1: Name the Configuration

Provide a name and description for the File and Folder Operation configuration.

Step 2: Define Configuration

You can perform the following actions:

- Copy Files and Folders
- Rename/Move Files and Folders
- Delete Files and Folders

Copy Files and Folder

To copy files and folders, select the *Copy* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: • *Copy a File* - To copy a file from one location to another • *Copy a File to a Folder* - To copy a file from one location to a specified folder • *Copy Multiple Files* - To copy multiple files to a specified folder • *Copy a Folder* - To copy a folder from one location to another
Source File	Specify the file that has to be copied. The file can either be in a shared location or in the specified location in the client machines.
Destination File	Specify the destination location with the file name.
Destination Folder	Specify the destination folder to copy the files/folders.

Parameter	Description
Include Read Only Files	Select this option, if you wish to copy the files even if it has only read-only permissions
Include System Files	Select this option if you wish to copy the system files.
Include Hidden Files	Select this option if you wish to copy the hidden files.
Overwrite Existing Files	Select this option to overwrite the existing files.
Create Destination Directory if doesn't Exist	Select this option to create the destination directory, if it does not exist.
Include Sub Folders	Select this option, if you wish to copy sub folders or the files within the sub folders.
Continue on Error	While copying multiple files or folders, specify whether to continue, if any error is encountered while copying.
Choose file modification time	Specify the file or folder modification time. Files that meet the specified criteria will only be copied.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Rename / Move Files and Folders

To rename or move the files and folders, select the *Rename/Move* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: • Rename/Move a file • Rename/Move a folder
Source File/Folder	Specify the file or the folder that has to be copied
Destination File/Folder	Specify the destination file or the folder.

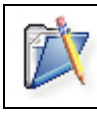
Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Delete Files and Folders

To delete the files and folders, select the *Delete* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: • Delete a File • Delete Multiple Files • Delete a Folder
Source File	Specify the files/folders that has to be deleted

Include Read Only Files	Select this option, if you wish to delete the read-only files
Include System Files	Select this option, if you wish to delete the system files
Include Hidden Files	Select this option, if you wish to delete the hidden files.
Include Sub Folders	Select this option, if you wish to delete the sub folders or the files within the sub folders.
Continue on Error	While deleting multiple files or folders, specify whether to continue, if any error is encountered while deleting.



Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

To modify a file action from the **List of File Actions** table, select the appropriate row and click icon and change the required values.

To delete a file action from the **List of File Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the File and Folder Operation Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined File and Folder Operation Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Windows XP Firewall

Configuring Windows XP Firewall

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Firewall configuration in the Windows XP Operating System can be modified using Desktop Central. The Windows XP Firewall blocks or permits access to the computer for specific TCP or UDP ports.

Note: The Firewall Configuration can be deployed only on the computers with the Windows XP (with Service Pack 2) Operating System.

Step 1: Name the Configuration

Provide a name and description for the Firewall Configuration.

Step 2: Define Configuration

Select the Firewall Action from the combo box. The action could be any of the following:

- **ON**: To turn on the Windows XP Firewall.
- **OFF**: To turn off the Windows XP Firewall.
- **DONT MODIFY**: To preserve the client settings. This option is selected by default.

Note: The Firewall configurations defined using Desktop Central can be deployed successfully to the client computers. However, it will take effect only when you turn on the Windows XP Firewall.

Specify the following parameters to block/unblock a port:

Parameter	Description
Port Action	Select whether to block, unblock, or to retain client settings using the Windows XP Firewall. The default option is Block.
Choose Port [Number - Name - Protocol]	Specify the port in the form of Port Number - Port Name - Protocol. The standard ports and services are listed in the combo box. If the required port is not listed, select the **Customize** link to either choose the port from the Additional ports list or to add your own by providing the required details.
Dependent Services	On selecting the port the dependent services are shown in this field. This cannot be modified from here.

Note:

1. To block/unblock more ports, click **Add More Ports** and repeat Step 2. The port gets added to the **Firewall** table.
2. To modify a setting from this table, select the appropriate row, click icon and change the required values.
3. To delete a setting from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets deploying the Firewall Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Firewall Configuration in the defined targets. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring General Computer Settings

Configuring General Computer Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The General Configuration is for configuring the general settings for the computers, such as configuring display the last user name, synchronize the system time with Time Server, and so on.

Step 1: Name the Configuration

Provide a name and description for the General Configuration.

Step 2: Define Configuration

The table below lists the general settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Display last User Name	To specify whether to display the previously logged user name or not. This is displayed when a user logs on to the system. To leave it unchanged, select *Preserve client settings* option.
Registered Owner*	The name of the registered owner of the system. This is displayed in the General tab of the My Computer properties window.
Registered Company*	The name of the company. This is displayed in the General tab of the My Computer properties window.
Time Server	Browse and select a time server to synchronize the time of the computer with of the time server. Time synchronization happens when the computer is started.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the General Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined General Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Managing Windows Local Groups

Managing Windows Local Groups

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Group Management allows you to add, modify, or delete local groups from the computers.

Step 1: Name the Configuration

Provide a name and description for the Group Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add Group
- Delete Group
- Modify Group

Add Group

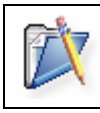
To add a group to the computer, select the **Add Group** link from the Choose Group Action table and specify the following:

Parameter	Description
Group Name	The name of the group that has to be created.
Description	The description of the group.
Add Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users or global groups that have to be added to the local group.
Overwrite if group already exist	Select this option, if you wish to overwrite the group definition, if one with the same name exists.

Note: If you wish to add more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

Delete Group

To delete a group from the computer, select the **Delete Group** link from the Choose Group Action table and specify the group name that has to be deleted.



Note: If you wish to delete more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

Modify Group

To modify a group of the computer, select the **Modify Group** link from the Choose Group Action table and specify the group name that has to be deleted.

Parameter	Description
Group Name	The name of the group that has to be modified.
Description	The description of the group.
Add Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users or global groups that have to be added to the local group.
Remove Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users to be removed from this group.

Note: If you wish to modify more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

To modify a setting from the **List of Settings** table, select the appropriate row and click icon and change the required values.

To delete a setting from the **List of Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Group Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Group Management Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Installing Patches

Installing Patches

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Install Patches configuration enables you to install patches to fix the application vulnerabilities from a central location.

Step 1: Name the Configuration

Provide a name and description for the Install Patches Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Add the Patches	Click the Add More Patches button to invoke the Patch Browser. From the patch browser select the patches that have to be applied. The patch browser has an option to view the missing patches or all patches, which can then be filtered based on the application and service pack.
Deployment Settings	Install After • Select this option and specify the date and time after which the patches have to be installed. The patches will be installed based on the Install Options selected after the scheduled time. Install Options • Install during computer startup: Select this option if the patches have to be deployed during computer startup. • Install during 90 minutes refresh interval: Select this option if the patches have to be installed after the computer startup when the next update happens (within 90 minutes) • Either of the above, whichever is earlier Reboot Policy • Do not reboot: Select this option if the client computers should not be rebooted after installing the patches. • Force Reboot when the user has logged in: Select this option to force the user to reboot the

Parameter	Description
	computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. • Force Shutdown when the user has logged in: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. • Allow user to skip Reboot: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. • Allow user to skip Shutdown:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Note: If you have reached this configuration page from the Patch Management tab by selecting the patches, the selected patches automatically gets added to the List of Patches.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Install Patches Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Install Patches Configuration in the defined targets. The software installation for the selected targets will happen during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Installing Software - MSI & EXE Packages

Installing Software - MSI & EXE Packages

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Software Installation configuration helps you to install MSI and EXE packages remotely to several computers of the Windows network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Software Installation Configuration.

Step 2: Define Configuration

You have an option to install either an EXE or an MSI package

- Install MSI Package
- Install EXE Package

Install MSI Package

Select the Installer type as **MSI** and specify the following values:

Parameter	Description
MSI Package Name	This will list all the MSI packages that are available in the Software Repository. Select the MSI that has to be installed.
Run As	The user as whom the MSI has to be installed.
Password	Password for the user as whom the MSI has to be installed.
Confirm Password	Confirm the password
Operation Type	To specify how the installation should happen. Select any of the following options: • *Install Completely:* Selecting this option will install the application automatically during next GPO update or user logon or system startup. • *Assign*: Selecting this option will create all the necessary shortcuts and registry entries. The application will be installed only when the user tries to open the application or during system startup, whichever is earlier. • *Remove*: Selecting this option remove (uninstall) the application from the system

Parameter	Description
	• *Redeploy*: Selecting this option will re-install the application.
Copy the Source File & Folder to client machines	Selecting this option will copy all the necessary installables to the client machines.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after system startup: • *During startup*: Select this option if the software has to be installed/uninstalled during computer startup. • *After startup*: Select this option if the software has to be installed/uninstalled after the computer startup when the next GP update happens (within 90 minutes) • *During or After Startup*: Either of the above, whichever is earlier
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here.
Reboot Policy	• *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. • *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. • *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. • *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. • *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Install EXE Packages

Select the Installer type as **EXE** and specify the following values:

Parameter	Description
EXE Package Name	This will list all the EXE packages that are available in the Software Repository. Select the EXE that has to be installed.
Run As	The user as whom the EXE has to be installed.
Password	Password for the user as whom the EXE has to be installed.
Confirm Password	Confirm the password
Operation Type	To specify how the installation should happen. Select any of the following options: • *Install:* Selecting this option will install the application automatically during next GPO update or user logon or system startup. • *Remove*: Selecting this option remove (uninstall) the application from the system
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: • *None:* Selecting this option will not copy the installation files. • *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. • *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation should happen during or after system startup.
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here.

Parameter	Description
Reboot Policy	• *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. • *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. • *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. • *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. • *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Windows Installer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Windows Installer Configuration in the defined targets. The software installation for the selected targets will happen as scheduled.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Installing Windows Service Packs

Installing Windows Service Packs

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Install Service Pack configuration enables you to install windows service packs to operating system and other windows applications from a central location.

Step 1: Name the Configuration

Provide a name and description for the Install Service Pack Configuration.

Step 2: Define Configuration

Specify the following:

Parameter	Description
Select the Service Pack	All the available Service packs are listed here. You can filter the view based on the OS or the application by selecting the appropriate option from the Select Application combo box. Select the service pack from the list and specify whether to reboot the system after applying the service pack.
Deployment Settings	Install After • Select this option and specify the date and time after which the service pack has to be installed. The service pack will be installed based on the Install Options selected after the scheduled time. Install Options • *Install during computer startup*: Select this option if the service pack has to be deployed during computer startup. • *Install during 90 minutes refresh interval*: Select this option if the service pack has to be installed after the computer startup when the next update happens (within 90 minutes) • Either of the above, whichever is earlier Reboot Policy • *Do not reboot*: Select this option if the client computers should not be rebooted after installing the service pack.

Parameter	Description
	• *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. • *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. • *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. • *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Note: If no service pack details are listed here, check whether you can configured the Proxy Settings.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Install Service Pack Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Install Service Pack Configuration in the defined targets. The software installation for the selected targets will happen during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring IP Printer

Configuring IP Printer

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The IP Printer Configuration is for adding or deleting the IP Printer connection in the computers. For configuring a shared or IP printers in the computer for specific users, refer to the Configuring Shared Printer / Configuring IP Printer topics under User Configurations.

Step 1: Name the Configuration

Provide a name and description for the IP Printer configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add an IP Printer
- Delete an IP Printer

Add an IP Printer

To add an IP Printer, select the **Action** as *Add* and specify the following values:

Parameter	Description
DNS Name/IP	The host name or IP address defined for the printer. *Example*: `192.111.2.32`
Printer Name	The display name for the printer.
Protocol	The printing protocol supported by the printer. Select the printing protocol from the Protocol list box. The default option is "RAW".
Port Number	The port number/queue name in which printing protocol is communicating between the computer and printer. Enter the port number in the Port Number field if the "RAW" Protocol is selected or enter the queue name if the "LPR" Protocol is selected. The default value is 9100.
Port Name	This is an optional field. By default, the port name is IP_<IP_Address/DNS_Name>. You can change the port name if required.
Shared Printer for Driver Installation	Browse to select a shared printer for installing the driver. If the drivers are already installed in the target computers, this field can be left blank.

Delete an IP Printer

To delete an IP Printer, select the **Action** as *Delete* and specify the following values:

Parameter	Description
Printer Name	The display name of the printer.
Delete all existing IP printer connections	To delete all the existing IP printer connections in the computer for the specified user, select this option.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the IP Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined IP Printer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Configuring Shared Printer

Launching Applications

Launching Applications

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Launch Application configuration enables you to launch an application during startup or shutdown of the computer.

Step 1: Name the Configuration

Provide a name and description for the Launch Application Configuration.

Step 2: Define Configuration

Select whether the application has to be launched from the local computer or from the network share. If you select the Local option, all the selected target computers should have the application in the same location. Specify the following:

Parameter	Description
Application Name*	Browse and select the application that has to be launched. The applications that are available in the local machine from where the application has to be launched can also be specified.
Arguments*	Specify the arguments for the application, if any.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note:

1. To launch more applications, click **Add More Application** and repeat Step 2. The added application gets added to the **Launch Application** table.
2. To modify an application from this table, select the appropriate row, click icon and change the required values.
3. To delete an application from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Launch Application Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Launch Application Configuration in the targets defined. The applications configured will be launched during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Displaying Legal Notices

Displaying Legal Notices

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The important enterprise wide announcements, legal notice, etc., can be configured using the Legal Notice configuration. The configured message will be displayed whenever the user presses ctrl+alt+del to login.

Step 1: Name the Configuration

Provide a name and description for the Legal Notice Configuration.

Step 2: Define Configuration

Specify the following:

Parameter	Description
Remove Already Defined Legal Notice	Select this option to clear the previous configurations, if any.
Window Title*	Specify the window title of the legal notice.
Message*	Specify the message that has to be displayed.

* - Click the icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Legal Notice Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Legal Notice Configuration in the defined targets. The configured legal notice will be displayed during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Displaying Message Box

Displaying Message Box

Displaying Message Box

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

For the computers in the network, the pop-up messages with the warning or error can be displayed during the system startup. If the system is already running while deploying this configuration, the message will be displayed during the system restart.

Step 1: Name the Configuration

Provide a name and description for the Message Boxes Configuration.

Step 2: Define Configuration

You have an option to create a new message box or delete the existing message box. Select the required option and specify the following:

Parameter	Description
Message Type	The message type as Information, Warning, or Error.
Window Title	The title of the message box.
Message	The message that has to be displayed.
Timeout in Seconds	The duration, in seconds, for the message display.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Message Boxes Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Message Boxes Configuration in the targets defined. The message will be displayed during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Displaying Legal Notices

Setting Path

 **Setting Path**

---

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Path is an environment variable that contains the path prefixes that certain applications, utilities, and functions uses to search for an executable file. The Path Configuration enables you to add path prefixes to this variable.

Step 1: Name the Configuration

Provide a name and description for the Path Configuration

Step 2: Define Configuration

Specify the path to be added to the environment variables. Multiple paths can be specified separated by a semi-colon (**;**). Click the ☆ icon to select and assign a dynamic variable to the Path variable.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Path Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Path Configuration in the targets defined. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Environment Variables

Managing Permissions

Managing Permissions

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Permission Management allows you to grant revoke permission on the files, folders and registry. Desktop Central Permission Management Configuration enables you to grant/revoke permissions to multiple computers from a central point.

Step 1: Name the Configuration

Provide a name and description for the Permission Management configuration.

Step 2: Define Configuration

You can grant or revoke permissions for the following objects:

- Files
- Folders
- Registry

Files

To grant or revoke permissions for files, select the *File* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: • Append - To append to the existing file permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. • Overwrite - To overwrite the existing file permissions • Revoke - To revoke the existing file

Parameter	Description
	permissions of the specified user/group. All the permissions to the specified user/group on that file will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the file for which you need to specify permissions
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Folders

To grant or revoke permissions for folders, select the *Folder* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: • Append - To append to the existing folder permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. • Overwrite - To overwrite the existing folder permissions • Revoke - To revoke the existing folder permissions. All the permissions to the specified user/group on that folder will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the folder for which you need to specify permissions
Inheritance	Select the required option to specify how the permission should effect its subfolders and files
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Registry

To grant or revoke permissions for registry, select the *Registry* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: • Append - To append to the existing registry permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. • Overwrite - To overwrite the existing registry permissions • Revoke - To revoke the existing registry permissions. All the permissions to the specified user/group on that registry key will be removed. However, the inherited permissions will not be removed.
Hive	Select the registry hive from the given options
Key	Specify the key within that hive for which you need to set the permissions
Inheritance	Select the required options to specify how the permission should effect its subkeys.
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

To modify a permission from the **List of Permission Actions** table, select the appropriate row and click icon and change the required values.

To delete a permission from the **List of Permission Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Permission Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Permission Management Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Registry Settings

Configuring Registry Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Registry Settings allows you to change the values in the registry in the workstations. Desktop Central Registry Settings Configuration enables you to modify the registry values from a central location.

Step 1: Name the Configuration

Provide a name and description for the Registry Settings Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Write Value
- Delete Value
- Add Key
- Delete Key

Write Value

To write a value to the registry, select the **Action** as *Write Value* and specify the following:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value.
Type	The type of the value. This varies with respect to the Header Key selected. Select the appropriate type from the combo box.
Value*	Specify the value to be added.
Data / Expression*	Specify the data or expression. If the new value has to be created without data, enter the word clear inside the parentheses as (clear).

* - Click the icon to select and assign a dynamic variable to this parameter.

	**Note**: If you wish to write more values, click **Add More Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Value

To delete a value from the registry, select the **Action** as *Delete Value* and specify the following values:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value.
Value	Specify the value to be deleted.

	**Note**: If you wish to delete more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Add Key

To add a registry key, select the **Action** as *Add Key* and specify the following:

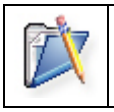
Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value to be added.

	**Note**: If you wish to add more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Key

To delete a registry key, select the **Action** as *Delete Key* and specify the following values:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value that has to be deleted.

	**Note**: If you wish to delete more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

To modify a registry setting from the **Registry Settings** table, select the appropriate row and click icon and change the required values.

To delete a registry setting from the **Registry Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Registry Settings Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Registry Settings Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Securing USB Devices

Securing USB Devices

---

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Secure USB Configuration is used to Enable or Disable the selected USB Devices in the computers. This configuration will be applicable to all the users of a partcular computer; provided the users do not have an individual USB configuration. For more information on USB Configuraton for users, refer to Secure USB under User Configurations.

Step 1: Name the Configuration

Provide a name and description for the Secure USB configuration.

Step 2: Define Configuration

Select the devices to be enabled/disabled from the given list:

- Mouse
- Disk Drive
- CD-ROM
- Portable Devices
- Floppy Disk
- Bluetooth
- Image
- Printer
- Modem

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Secure USB Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Secure USB Configuration in the targets defined. The configuration will take effect during the next system startup.
To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Securing USB for Users

Scheduling Tasks

Scheduling Tasks

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Windows Scheduler Configuration enables you to schedule any program, task, or a script to run at a specified time. You can also schedule a task to run daily, weekly, monthly , etc. The Scheduler Configuration enables you to add, modify tasks from a central point.

Step 1: Name the Configuration

Provide a name and description for the Scheduler Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Task
- Delete a Task

Create / Modify a Task

To create a new task, select the **Create Task** tab of the Scheduler Configuration. Select the **Modify Task** tab to modify an existing task. Specify the following values:

Parameter	Description
Name of the task*	The name of the task that has to be created/modified.
Overwrite if task already exits	Select this option to overwrite the task, if one with the same name exists. This option is only available for create task.
Application Name*	The application or the program that has to be run. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Arguments	The arguments to run the program, if any. Click the ☆ icon to select and assign a dynamic variable to this parameter.
User Name*	The name of the user as whom the task will be run. Click the ☆ icon to select and

Parameter	Description
	assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.
Confirm Password	Confirm the password again.
Perform this task*	Specify the time to perform the task. You can select from the following options: • *Daily:* To run the task daily. Specify the time and duration to run the task. • *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. • *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. • *Once:* To run the task only once. You need to specify the date and time. • *At System Startup:* To run the task when the system is started. • *At Logon:* To run the task during the user logon. • *When Idle:* To run the task when the system is idle for the specified time.
Advanced Settings	
General	• *Enabled*: Select this option to run the task at the specified time. • *Run only when logged on:* Select this option to run the task only when the user has logged on.
Scheduled Task Completed	• *Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. • *Stop Task:* Select this option and specify the duration after which the task will be stopped.
Idle Time	Select the required options: • Specify the duration,the system has to be idle before starting a task. • Stop the task if the computer ceases to be idle
Power Management	Select the required options: • Don't start the task if the computer is running on batteries • Stop the task if battery mode begins • Wake the computer to run this task

* - denotes mandatory parameters

If you wish to create/modify more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

Note: When a wrong password is provided for tasks scheduled in Win2k / WinXP SP1 machines, the tasks will be successfully created, but, fails to execute.

Delete a Task

To delete a task, select the Create Task tab of the Scheduler Configuration and specify the name of the task that has to be deleted.

If you wish to create/modify/delete more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

To modify a task from the **Task** table, select the appropriate row and click icon and change the required values.

To delete a task from the **Task** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Scheduler Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Scheduler Configuration in the defined targets. The scheduler configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Security Policies

Configuring Security Policies

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

For the computers in the network, the Security Policies are security settings to specify the security and restrictions. The security settings for preventing users to change file type association can be defined using **Security Policies Configuration**.

Step 1: Name the Configuration

Provide a name and description for the Security Policies Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Choose Policy Category	The specific policy area in which the security policy will be applied. Select the desired category from left. This displays the relevant security polices. For details on the each category, refer to Windows Help documentation. For details on the each policy in the **Select the Policy** list, refer to Security Policies topic.
Policy Value	To enable, disable, or to leave it unconfigured, select the appropriate option.

Note:

1. To modify a security policy from this table, select the appropriate row, click icon and change the required values.
2. To delete a security policy from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Security Policies Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Security Policies Configuration in the targets defined. The security policies will be applied during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Security Policies

Managing Shortcuts

Managing Shortcuts

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The shortcut is an icon that points to a file or folder. The Shortcut Configuration enables you to add shortcuts to the computers from a central point.

Step 1: Name the Configuration

Provide a name and description for the Shortcut Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create a Shortcut
- Delete a Shortcut

Create a Shortcut

To create a shortcut, select the **Action** as *Create Shortcut* and specify the following values:

Parameter	Description
Overwrite	To modify the existing shortcut select this option.
Shortcut Name*	Specify the name of the shortcut.
Target Application*	Browse and select the target application from the network for which a shortcut has to be created. The target application can also be in the local machine where the configuration is being deployed.
Arguments*	If the application requires any arguments, specify the arguments. Leave it blank if it does not require any arguments.
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: • *All Users Desktop*: Refers to the desktop common for all the users.

Parameter	Description
	• *All Users Start Menu*: Refers to the start menu common for all users. • *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. • *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Start In Folder*	Some applications may have some references to additional files during execution. In such cases, browse and select the location from where the application has to be started.
Shortcut Comments	Specify the comments for this shortcut.
Icon File*	Browse and select the icon for the shortcut.
Run Window	Select how the application has be started - *Normal*, *Maximized*, or *Minimized*.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to create more shortcuts, click **Add Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

Delete a Shortcut

To delete a shortcut, select the **Action** as *Delete Shortcut* and specify the following values:

Parameter	Description
Shortcut Name	Specify the name of the shortcut. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Shortcut Location	Select the location from where the shortcuts needs to be deleted. The shortcut location can be any of the following: • *All Users Desktop*: Refers to the desktop common for all the users. • *All Users Start Menu*: Refers to the start menu common for all users. • *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. • *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

Note: If you wish to delete more shortcuts, click **Add More Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

To modify a shortcut from the **Shortcut** table, select the appropriate row and click  icon and change the required values.

To delete a shortcut from the **Shortcut** table, select the appropriate row and click  icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shortcut Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shortcut Configuration in the defined targets. The shortcut configuration will take effect during the next system start up.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Windows Services

Configuring Windows Services

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Applications that have to be run automatically whenever the system is started can be configured to run as a Windows service. However in certain cases, after installing an application as a service, you may wish to change the startup type or delete the service. The Service Configuration enables you to change the settings for the services available in the **Control Panel >Administrative Tools >Services**.

Step 1: Name the Configuration

Provide a name and description for the Service Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Service Name	Select the name of the service from the combo box. The combo box contains the list of standard Windows services. If the required service is not listed, click **Customize** to either select the service from the Additional Services list or add you own by giving the required details.
Action	Specify the action to be performed from the following: • *Don't Modify*: To preserve the client settings. This option is selected by default. • *Start*: Select this option to start the service. • *Stop*: Select this option to stop the service. • *Restart*: Select this option to restart the service.
Service Startup Type	Select how the service should be started from the following options: • *Don't Modify*: To preserve the client setting. • *Manual*: Select this option if the service has to be manually started after the system startup. • *Disabled*: Select this option to disable the service. • *Automatic*: Select this option to automatically start the service along with the system.

Note:

1. To add more services, click **Add More Service** and repeat Step 2. The service gets added to the **Services** table.
2. To modify a service from this table, select the appropriate row, click icon and change the required values.
3. To delete a service from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Service Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Service Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Managing Windows Local Users

Managing Windows Local Users

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The User Management allows you to add, modify, or delete local users from the computers.

Step 1: Name the Configuration

Provide a name and description for the User Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add User
- Change Password
- Remove User
- Modify User

Add User

To add an user to the computer, select the **Add User** link from the Choose User Action table and specify the following:

Parameter	Description
User Name	The user name for the user to be created.
Full Name	The full name of the user.
Description	The description for this user.
Password	The password for this user.
Confirm Password	Confirm the password again.
Overwrite if user already exist	Select this option to overwrite the user, if one with the same name exists.
Advanced Settings	
User Must change password at next logon	Specify whether the user has to change the password during the next logon or not.
User Cannot Change Password	Specify whether the user can change the password or not.
Password Never Expires	Specify whether the password should expire or

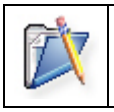
Parameter	Description
	not.
Account is Disabled	Specify whether the user account should be disabled or not.
User Profile	
Member of	Specify the groups in which this user account is a member.
Logon Script	Specify the logon script that has to be executed during the user logon.
Profile Path	Specify the path where the user profiles has to be stored.
Local Path	Specify a local path as the home folder. For example, c:\users\johnsmith.
Connect Map To	If the user's home folder has to be stored in a network directory, select the drive letter in the **Connect Map** and specify the network path in the **To** field.

Note: If you wish to add more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Change Password

To change the user password, select the **Change Password** link from the Choose User Action table and specify the following:

Parameter	Description
User Name	The user name of the user whose password has to be changed.
Password	Type the new password.
Confirm Password	Re-type the password to confirm.



Note: If you wish to continue adding more actions, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Remove User

To remove an user from the computer, select the **Remove User** link from the Choose User Action table and specify the user to be removed.

Note: If you wish to remove more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Modify User

To modify an user, select the **Modify User** link from the Choose User Action table and specify the following:

Parameter	Description
User Name	The user name of the user to be modified.
Full Name	The full name of the user.
Description	The description for this user.
Advanced Settings	
User Must change password at next logon	Specify whether the user has to change the password during the next logon or not.
User Cannot Change Password	Specify whether the user can change the password or not.
Password Never Expires	Specify whether the password should expire or not.
Account is Disabled	Specify whether the user account should be disabled or not.
Account is Locked	Specify whether the user account should be locked or not.
User Profile	
Member of	Specify the groups in which this user account is a member.
Logon Script	Specify the logon script that has to be executed during the user logon.
Profile Path	Specify the path where the user profiles has to be stored.
Local Path	Specify a local path as the home folder. For example, c:\users\johnsmith.
Connect Map To	If the user's home folder has to be stored in a network directory, select the drive letter in the **Connect Map** and specify the network path in the **To** field.

Note: If you wish to modify more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

To modify a setting from the **List of Settings** table, select the appropriate row and click icon and change the required values.

To delete a setting from the **List of Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the User Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined User Management Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Collections

1. Define Collection
2. Define Target
3. Save or Deploy Collection

A collection of Configurations can be deployed in the target client workstation using Desktop Central. The advantages of Collection are

- The targets are defined once for multiple Configuration.
- When the configuration is deployed, it saves time to apply the configuration since collection of configuration is applied in each workstation.

Step 1: Define Collection

1. Click Add Collection link from the Quick Links.
2. Select the collection type as User Collection or Computer Collection. This opens the Add Collection Wizard.
3. Provide a name and description for the collection.
4. Choose the configurations that have to added to this collection and click Next. The configurations are specific to the collection type you have selected above.
5. Define the chosen configurations. Refer to User Configurations and Computer Configurations sections for details about the configurations.

Step 2: Define Target

Select the targets for which the configurations have to be applied. Refer to the Defining Targets topic for more details.

Step 3: Save or Deploy Collection

After defining the configurations and targets, click **Finish** to deploy the defined configurations to the selected targets. You also have an option to save the configurations as drafts for later modifications by clicking the **Save as Draft** button.

Note: The collections that are saved as drafts will not be deployed. You have to modify the definition and deploy it later.

Defining Targets

- Selecting Targets from a Domain
- Selecting Targets from a Workgroup
- Selecting Targets in Remote Offices
- Modifying a target in Target List
- Deleting a target from the Target List

After defining the configuration, the configuration has to be deployed in the target client workstations. The target client workstations have to be defined for the configurations individually. Defining the targets involves selecting various types of targets given below:

The targets must be defined to deploy the Configuration in the machines of the network. When you add a configuration or collection of Configuration, you can find "Step 2" as **Define Target** in the GUI or in this documentation. This section explains the procedure to define the target for a configuration or collection of Configuration.

To define the targets for deploying the configuration or collection, the targets must be added to the **Target List**. A target can be added, removed or modified in the **Target List**.

Selecting Targets from a Domain

To add target computers and users from a Active Directory based domain, follow the steps below:

1. Select a domain from the list.
2. You can deploy the configuration to any of the following:
    1. **Site** - to deploy the configuration to all the users/computers of that site.
    2. **Domain** - to deploy the configuration to all the users/computers of that domain.
    3. **Organizational Unit** - to deploy the configuration to all the users/computers of that OU.
    4. **Group** - to deploy the configuration to all the users/computers of that Group.
    5. **User/Computer** - to deploy the configuration to the specified users/computers.
    6. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
    7. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.

3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different domains, use the **Add More Targets** button to add targets from multiple domains.

Selecting Targets from a Workgroup

To add target computers and users from a workgroup, follow the steps below:

1. Select a workgroup from the list.
2. You can deploy the configuration to any of the following:
    1. **Workgroup** - to deploy the configuration to all the users/computers of that workgroup.
    2. **User/Computer** - to deploy the configuration to the specified users/computers.
    3. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
    4. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.
3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different workgroups, use the **Add More Targets** button to add targets from multiple workgroups.

Selecting Targets in Remote Offices

To add target computers and users from remote offices, follow the steps below:

1. Select a remote office from the list. The remote office can either be a domain or a workgroup.
2. You can deploy the configuration to any of the following:
    1. **Site** - to deploy the configuration to all the users/computers of that site. This option is only available if the selected remote office is a domain.
    2. **Remote Office** - to deploy the configuration to all the users/computers of that remote office.
    3. **Organizational Unit** - to deploy the configuration to all the users/computers of that OU. This option is only available if the selected remote office is a domain.
    4. **Group** - to deploy the configuration to all the users/computers of that Group. This option is only available if the selected remote office is a domain.
    5. **User/Computer** - to deploy the configuration to the specified users/computers.
    6. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by

selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.

7. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.

3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different remote offices, use the **Add More Targets** button to add targets from multiple domains.

Filter the selected target

You can exclude certain parts of the network which does not require the configuration to be deployed. This is optional when defining the targets. Desktop Central provides the option to exclude the parts of the Windows network. Select the Exclude Target check box to view the available options:

Exclude if Target Type is

The target types can be excluded which are in the lower hierarchy to the target selected in the **Select the target type and define** field. The target type can be excluded using the **Browse** button. Click the **Browse** button next to the required target types under the **Exclude if Target Type is** field to launch **Network Browser** window. Select the target type to be excluded for configuration deployment and click **Select** button. This field is mandatory. The target type can be any of the following (varies based on the target options selected):

- Branch - The branch offices to be excluded
- Domain - The domains to be excluded
- Organization Unit - The OUs to be excluded
- Group - The groups to be excluded
- Computer - The computers to be excluded
- IP Address - The IP Addresses to be excluded
- IP Range - The range of IP Addresses to be excluded
- Custom Group - The custom groups to be excluded

Exclude if Operating System is

The targets with specific Windows OS can be excluded for configuration deployment. Select the options under the **Exclude if Operating System is** field which has to excluded for configuration deployment.

Exclude if Machine Type is

The targets with specific machine type such as Notebook, Tablet PC, Desktop, Member Server, TermServClient, or Domain Controller can be excluded for configuration deployment. Select the options under the **Exclude if Machine Type is** field which has to excluded for configuration deployment.

Modifying a Target

To modify a target in the Target List, follow these steps:

1. Select the  button under **Actions** column in the desired row that has to modified.
2. Change the targets as required and click the **Modify Target** button. The target details are updated in **Target List**.

Deleting a Target

To delete a row in the **Target List**, select the  button under **Actions** column next to target that has to removed.

Managing Configurations and Collections

- Viewing the Status of Configuration/Collection
- Modifying the Configuration/Collection
- Suspending the Configuration/Collection
- Resuming the Suspended Configuration/Collection

Clicking the **View Configuration** from the Quick Links will list the details of the configurations and collections that are defined using Desktop Central. You can view the details of the configurations by clicking the corresponding configuration name. Apart from viewing the configuration details, you can perform the following actions:

- Modify the Configuration/Collection
- Suspend a Configuration/Collection
- Resume a suspended Configuration/Collection

Viewing Status of Configuration / Collection

To view the status of the defined configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. The status column provides the current status of the configuration/collection. The table given below lists the various states of the configuration/collection and its description:

Status	Description
Draft	Represents the configurations/collections that are saved as draft.
Ready To Execute	Represents the configurations/collections that are ready for execution. This will be the initial state of the deployed configurations/collections.
In Progress	Represents that the configuration is applied on one or more targets. Will continue to remain in this state until the configurations are applied to all the defined targets.
Suspended	Represents that the configuration/collection has been suspended.
Executed	Represents that the configuration/collection has been applied to all the defined targets.

3. To view the status of the configurations on individual targets, click the configuration name.

Modifying the Configuration / Collection

To modify a configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. Click the icon from the Actions column of the corresponding configuration/collection.
3. Change the values as required.
4. Click **Deploy**.

Suspending the Configuration / Collection

To suspend a configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. Click the icon from the Actions column of the corresponding configuration/collection that has to be suspended.

	**Note:** Configurations that have been applied to targets prior to suspension will not be reverted. Suspending a configuration will only stop further deployments.

Resuming the Suspended Configuration / Collection

To resume a suspended configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. Click the icon from the Actions column of the corresponding configuration/collection that has to be resumed.

Viewing System Uptime Report

- Configuring Data Storage Period
- Viewing Report for a Specified Period
- Viewing Detailed Uptime Report
- Exporting the Report

Provides the total uptime and downtime of the computers in the network for a given period. The report can be filtered to view computers in a specific domain and period. To view the report, select **Reports --> Power Management Reports --> System Uptime Report**

Configuring Data Storage Period

Desktop Central, by default, stored the uptime/downtime details of all the computers for a period of 30 days. This can be configured to suit your need. To specify the period,

1. Click Edit Settings link. This is open the Power Report Settings dialog.
2. Specify the number of days you wish to store the data and click Apply.

Viewing Report for a Specified Period

1. Select the Domain or select All Domains to view the uptime of all the computers.
2. Select a period from the list. To specify a custom period, click Select Custom Date and specify the start and end dates.
3. Specify the start and end time for which the report has to be displayed. If you wish to see the complete details, specify the start and end time as 00:00 and 23:59 respectively.
4. Selecting the "Consider hibernate/standby as shutdown" option will show the hibernate/standby periods as downtime.
5. Click Apply Fileter to view the report based on the specified criteria.

Viewing Detailed Uptime Report

Desktop Central will display the summary view of the total uptime and downtime of the computers based on the selected criteria. Selecting the Detail Report option will display the start and shutdowm times of the computers for the given period. You can also click the computer name to view its detailed and summary reports.

Exporting the Report

The System Uptime Report can be exported to a PDF or a CSV format by clicking the respective options from the top-right. The current report that is being displayed will be exported to the selected format.

Viewing Configuration Reports

The Configuration reports helps the administrators to view the details of the configurations that are applied on users, computers, and based on the configuration type. To view the reports, follow the steps given below:

1. Click the **Reports** tab to invoke the **Reports** page.
2. Click the desired report from the Configuration Reports.

The Configuration Reports includes the following reports:

- Configuration by User
- Configuration by Computer
- Configurations by Type

Configuration by User

This report provides a list of users for whom configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for a particular user and the last configuration and time at which it was applied. Clicking the user name will list the details of the configurations applied for that user.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configuration by Computer

This report provides a list of computers for which configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for that computer and the last configuration and time at which it was applied. Clicking the computer name will list the details of the configurations applied for that machine.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configurations by Type

This report provides you the list of configurations that have been applied on users and computers based on the configuration type. It also provides you the total number of configurations that have been applied for a particular type and the last configuration, and time at which it was applied.

Configuration Templates

Configuration Templates

Templates are predefined configurations that help in achieving a specific task. While you can perform any of these configurations by defining them on your own, templates helps to get things done faster. The following are advantages of Templates over the normal configurations:

1. Helps to complete the configurations quickly.
2. You do not need to know how to achieve a specific task; just need to select the target computers to apply the configuration.
3. You does not have to explore all the supported configurations and then select to define.

Using Templates

To view the available templates, select the Admin tab and click the Templates link from the left. This will list all the templates provided by Desktop Central. You can also filter the view by selecting an appropriate category from the combo box. The Type column indicates whether the configuration is applied to Users or Computers. The templates are tagged as below:

- Control Panel
- Hard Disk Maintenance
- Internet Explorer
- Network
- Power Management
- Proxy Configuration
- Restrict Media
- Security
- Service Management
- System Tools
- USB Security
- User Management
- XP Firewall Management

To use the template, follow the steps below:

1. Select Admin --> Templates to view the templates.
2. Click the Template that has to be applied to view its details; click the **Create from Template** button to create the configuration. Clicking **Create Configuration** link will also do the same action. This opens the configuration with all the properties defined.
3. Using the Defining Targets procedure, define the targets for deploying the configuration.
4. Click the **Deploy** button to deploy the defined Configuration in the targets defined. To save the configuration as draft, click **Save as Draft**.

Supported Templates

Desktop Central supports various templates that can be applied to Users/Computers. Follow the links below to view the details of the templates:

- Computer Configuration Templates
- User Configuration Templates

Computer Configuration Templates

Computer Configuration Templates

- Change local admin account password
- Cleanup Recycle bin to free-up Hard Disk space
- Create Alternate local Admin Account
- Defrag Hard Disk for performance
- Delete local Administrator Account
- Disable the USB drives
- Disable Unused local Guest account
- Open MEDC ports for communication
- Restrict CD-ROM access
- Restrict Floppy Access to locally logged on users
- Scan and Fix Hard disk Errors
- Start MEDC Agent Service
- Write Protect the USB Storage Devices

Change local admin account password

To enhance the security, the administrators will prefer to change the password periodically. This template enables you to change the password of the local administrator account in the client machines.

Cleanup Recycle bin to free-up Hard Disk space

This helps in freeing up the hard disk space by removing the unwanted files/data from 18 different locations.

Create Alternate local Admin Account

To keep the computers secured, the administrators will prefer to change the local administrator account periodically. This template enables you to create an alternate local administrator account in the client computers.

Defrag Hard Disk for performance

A fragmented disk reduces the performance. It is recommended to defragment the disk periodically to improve the hard disk performance.

This template enables defragmentation of the hard disk at the scheduled time.

Delete local Administrator Account

This template enables you to delete the local administrator account in the client computers.

Disable the USB drives

To prevent data theft, the administrators prevent the users from using USB drives. This template, when applied to client computers, prevent them from using the USB drives.

Disable Unused local Guest account

Unused guest accounts are vulnerable points for the hackers. It is recommended to delete or disable any unused guest accounts from the client computers to avoid any misuse.

This template helps to disable the unused guest accounts from the client computers.

Open MEDC ports for communication

Desktop Central requires port 8021 for agent server communications and port 6100 for Remote Desktop Sharing. These port should not be blocked by the Windows Firewall for smooth functioning.

This template, when applied to client computers, will open up these ports to enable proper communication between the agent and server.

Restrict CD-ROM access

This template restrict the users form accessing the CD-ROM drives.

Restrict Floppy Access to locally logged on users

Allowing locally logged on users to access the floppy drives is a vulnerable point for hacking. Administrators prefer to disable access to the floppy drives when the users have not logged on to the domain.

This template helps in restricting the locally logged on uses to access the floppy drives.

Scan and Fix Hard disk Errors

The hard disks have to be periodically scanned for any errors and fix them. This will improve the life and performance of the disk.

This template enables scanning and fixing the hard disk errors in the client machines at the scheduled time.

Start MEDC Agent Service

When Scope of Management is defined, Desktop Central agent is installed in all the client computers that are within the scope. The Desktop Central agent has to be running as a service in the client computers to ensure proper communication with the Desktop Central Server.

This template helps you to start the Desktop Central Agent service in the client computers.

Write Protect the USB Storage Devices

To prevent data theft, the administrators prevent the users from writing data to USB storage devices. This template, when applied to client computers, prevent them from writing any data to the USB storage devices.

User Configuration Templates

 **User Configuration Templates**

- Restrict Network Connections
- Restrict Control Panel Applets
- Proxy configuration for Internet Explorer
- Laptop Power Saver Scheme
- IE Browser restrictions for clients
- Disable Control Panel

Restrict Network Connections

Network properties when changed by the user result in bad network connectivity and unnecessary help desk calls in resolving the problem. This could be avoided by restricting the users from changing the network properties.

This template, when applied to users, will prevent them from changing the network properties.

Restrict Control Panel Applets

To enhance the security, the administrators can restrict the users from accessing specific Control Panel applets. This includes, Add/remove programs, Add/remove hardware, Internet options, Power options and System applet.

Proxy configuration for Internet Explorer

This template can be used to configure proxy server settings in the Internet Explorer browser of the client machines.

Laptop Power Saver Scheme

Establishing correct power settings helps in saving energy costs substantially. This template provides the recommended power settings for Laptops.

IE Browser restrictions for clients

This template restricts users from changing the Internet Explorer settings like Connections, Content, Favorites, Programs, Security, Advanced, History and Save As options

Disable Control Panel

You can use this template to disable the Control Panel completely. When applied to users, the users will not be able to access the Control Panel.

User Logon Reports

How are these reports generated?

These reports are generated with the help of the Desktop Central Agents installed in the client systems to track the user logon details

What way does it differ from Active Directory Reports?

In the case of Active Directory reports, if multiple domain controllers are used, the synchronization of data between the domain controllers happens at regular intervals and not very frequently. Hence the reports derived from the Active Directory may not be the latest or actual. To provide the current reports of the logon details, Desktop Central agent is used.

In addition to the current details, it also provides the logon history details, which is not available in the Active Directory reports.

Is there any limitation?

Yes, these reports are available only to the users and computers that fall within the defined scope of management. Also, when an user logs in and logs out immediately, this may not be tracked.

- Setting Up User Logon Reports
- Viewing User Logon Reports

Viewing User Logon Reports

Viewing User Logon Reports

To view the User Logon Reports, select the Reports tab and click the User Logon Reports link from the left pane. The User Logon Reports are classified under the following headings; click the links to learn more:

- General Reports
- Usage Reports
- History Reports

General Reports

 **General Reports**

Currently Logged on Users

Provides the list of users who are currently logged on to the domain.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Currently Logged on Users** link available under the General Reports category.

Currently Logged on Computers

Provides the list of computers from where users have logged on to the domain.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Currently Logged on Computers** link available under the General Reports category.

Usage Reports

 **Usage Reports**

Computers with No User Logon

Provides the list of computers where no user have logged on.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Computers with No User Logon** link available under the Usage Reports category.

History Reports

 **History Reports**

- User Logon History
- User Logon History by Computers
- Domain Controllers with Reported Users
- User Logon History on Domain Controller

User Logon History

Provides the list of history of users who have logged on to the domain in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History** link available under the History Reports category.

User Logon History by Computers

Provides the list of computers and their corresponding user logon history in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History by Computers** link available under the History Reports category.

Domain Controllers with Reported Users

Provides the list of users and their corresponding Domain Controllers (logon servers) in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Domain Controllers with Reported Users** link available under the History Reports category.

User Logon History on Domain Controller

Provides the list of domain controllers and their corresponding user logon history in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History by Domain Controllers** link available under the History Reports category.

Active Directory Reports

Desktop Central gives you an insight into the Active Directory by providing reports on various Active Directory components. The reports can be accessed by selecting the Reports tab from the client window. The following reports about the Active Directory are shown:

- Active Directory User Reports
- Active Directory Computer Reports
- Active Directory Group Reports
- Active Directory Organization Unit Reports
- Active Directory Domain Reports
- Active Directory GPO Reports

More granular reports are provided for each of the above components.

Active Directory Report Features

- Ability to generate reports for custom inputs for granularity.
- Customizable columns in all the reports.
- Columnar sorting of reports
- Export reports in PDF and CSV formats.
- Ability to synchronize report data with Active Directory at regular intervals.

Active Directory User Report

Active Directory User Report

To access the User Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page. The User Reports is selected by default.
2. Select the required link to view the reports.

Follow the links to learn more about the various User Reports provided by Desktop Central

- Active Directory General User Reports
- User Account Status Reports
- Password Based User Reports
- Privileged User Reports
- Logon Based User Reports

Active Directory General User Reports

 **Active Directory General User Reports**

- All User Accounts
- Recently Created User Accounts
- Recently Modified User Accounts
- User Accounts without Logon Scripts
- User Accounts in Multiple Groups
- User Accounts that Never Expires

All User Accounts

Provides the details of all the users of the domain that the system/user running the Desktop Central belongs to.

To view the report, click the **All User Accounts** link available under the General Reports category. Clicking a user from the report displays the complete user information of that user.

Recently Created User Accounts

Provides the details of the user accounts that are created recently. This is determined based on the value contained in the *createTimeStamp* attribute of the Active Directory.

To view the report, click the **Recently Created User Accounts** link available under the General Reports category.

By default, the users created for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

Recently Modified User Accounts

Provides the details of the user accounts modified recently. This is determined based on the value contained in the *modifyTimeStamp* attribute of the Active Directory.

To view the report, click the **Recently Modified User Accounts** link available under the General Reports category.

By default, the user accounts modified for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

User Accounts without Logon Scripts

Provides the details of the users who do not have any scripts executed during their logon to the domain. This is determined based on the value contained in the *scriptPath* attribute of the Active Directory.

To view the report, click the **User Accounts without Logon Scripts** link available under the General Reports category. Clicking a user from the report displays the complete information of that user.

User Accounts in Multiple Groups

Provides the details of the user accounts that are in more than one groups. This also includes the nested groups i.e., groups that contain other groups as its members in the domain.

To view the report, click the **User Accounts in Multiple Groups** link available under the General Reports category.

User Accounts that Never Expires

Provides the list of user accounts that never expires. This is determined based on the value contained in the *userAccountControl* of the Active Directory.

To view the report, click the **User Accounts that Never Expires** link available under the General Reports category.

User Account Status Reports

User Account Status Reports

- Active User Accounts
- Inactive User Accounts
- Disabled User Accounts
- Locked User Accounts
- Expired User Accounts

Active User Accounts

Provides the list of users who have logged on to the domain in the past 30/60/90/180 days. This is determined based on the value contained in the *lastLogon* attribute of the Active Directory.

To view the report, click the **Active User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Inactive User Accounts

Provides the list of users who have not logged on to the domain in the past 30/60/90/180 days. This is determined based on the value contained in the *lastLogon* attribute of the Active Directory.

To view the report, click the **Inactive User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Disabled User Accounts

Provides the list of user accounts that are disabled by the administrator. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Disabled User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Locked User Accounts

Provides the details of the user accounts that have been locked out. The user account will get locked on frequent bad login attempts. The Account Lock Out Policy specifies the allowed number of bad login attempts after which the account will be locked. The account will be automatically unlocked after sometime. The locked user accounts are determined based on the value contained in the *lockoutTime* attribute of the Active Directory.

To view the report, click the **Locked User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Expired User Accounts

Provides the details of the user accounts that have expired. This is determined based on the value contained in the *accountExpires* attribute of the Active Directory.

To view the report, click the **Expired User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Password Based User Reports

Password Based User Reports

- Soon-to-Expire User Passwords
- Password Expired User Accounts
- Password Never Expiring User Accounts
- User Accounts Password that cannot be Changed

Soon-to-Expire User Passwords

Provides the details of the users whose password will expire within the specified number of days. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Soon-to-Expire User Passwords** link available under the Password Based Reports category.

By default, the users whose passwords will expire in another seven days is shown. You can select a different period to view the report. Clicking a user from the report displays the complete information of that user.

Password Expired User Accounts

Provides the details of the users whose password has expired. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Password Expired User Accounts** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

Password Never Expiring User Accounts

Provides the list of users whose password never expires. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Password Never Expiring User Accounts** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

User Accounts Password that cannot be Changed

Provides the list of users who cannot change their password. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **User Accounts Password that cannot be Changed** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

Privileged User Accounts

 **Privileged User Accounts**

- Domain Admin User Accounts
- User Accounts with Dial-in Permissions

Domain Admin User Accounts

Provides the list of users who have domain administrative privileges.

To view the report, click the **Domain Admin User Accounts** link available under the Accounts with Privileged User Accounts category.

User Accounts with Dial-in Permissions

Provides the list of users who have dial-in permissions to access the domain. This is determined based on the value contained in the *msNPAllowDialinattribute* of the Active Directory.

To view the report, click the **User Accounts with Dial-in Permissions** link available under the Privileged User Accounts category.

Logon Based User Reports

 **Logon Based User Reports**

- Unused User Accounts
- Recently Logged On User Accounts
- Last Logon Failed User Accounts

Unused User Accounts

Provides the list of users who have not logged on to the domain since creation of the account. This is determined based on the value contained in the *lastLogon* of the Active Directory.

To view the report, click the **Unused User Accounts** link available under the Logon Based Reports category. Clicking a user from the report displays the complete information of that user.

Recently Logged On User Accounts

Provides the details of the users who have logged on in the past n days. The recently logged on users are determined based on their last logon time.

To view the report, click the **Recently Logged On User Accounts** link available under the Logon Based Reports category.

By default, the users logged on for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

Last Logon Failed User Accounts

Provides the list of users whose last logon has failed. This is determined based on the value contained in the *badPasswordTime* and *badPwdCount* attributes of the Active Directory.

To view the report, click the **Last Logon Failed User Accounts** link available under the Logon Based Reports category. Clicking a user from the report displays the complete information of that user.

Active Directory Computer Reports

Active Directory Computer Report

To access the Computer Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Computer Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Computer Reports provided by Desktop Central

- General Computer Reports
- Server Based Reports
- Computer OS Based Reports

General Computer Reports

General Computer Reports

- All Computers
- Windows Workstation
- Recently Added Computers
- Recently Logged On Computers
- Recently Modified Computer Accounts
- Disabled Computer Accounts
- Computer Accounts by OU

All Computers

Provides the list of all the computer accounts available in the domain.

To view the report, click the **All Computers** link available under the General Reports category. Clicking a computer account from the report displays the complete information of that account.

Windows Workstation

Provides the details of the workstations in the domain. All the computers except Servers and Domain Controllers are termed as workstations.

To view the report, click the **Windows Workstation** link available under the General Reports category. Clicking a computer account from the report displays the complete information of that account.

Recently Added Computers

Provides the details of the computer objects that are created recently. This is determined based on the value contained in the *createTimeStamp* attribute.

To view the report, click the **Workstations** link available under the General Reports category.

By default, the report displays the computer accounts that are created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Recently Logged On Computers

Provides the list of computer accounts through which an user has logged on to the domain. This is determined based on the value contained in the *lastLogon* attribute.

To view the report, click the **Recently Logged On Computers** link available under the General Reports category.

By default, the report displays the computer accounts through which an user has logged on to the domain in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Recently Modified Computer Accounts

Provides the details of the computer objects that are modified recently. This is determined based on the value contained in the *ModifyTimeStamp* attribute.

To view the report, click the **Recently Modified Computer Accounts** link available under the General Reports category.

By default, the report displays the computer accounts that are modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Disabled Computer Accounts

Provides the list of computer accounts that are disabled in the domain. This is determined based on the value contained in the *userAccountControl* of the Active Directory.

To view the report, click the **Disabled Computer Accounts** available under General Reports category. Clicking a computer account from the report displays the complete information of that account.

Computer Accounts by OU

Provides the list of computer accounts filtered by the OU it belongs to.

To view the report, click the **Computers Accounts by OU** available under General Reports category.

By default, the computer accounts of all the OUs in the domain are listed. Browse to select a specific OU and click **Generate** to view the computer accounts of that OU. Clicking a computer account from the report displays the complete information of that account.

Server Based Reports

Server Based Reports

- Windows Servers
- Member Servers
- Domain Controllers

Windows Servers

Provides the list of Windows Servers in the domain. This is determined based on the value contained in the *operatingSystem* attribute of the Active Directory.

To view the report, click the **Windows Servers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Member Servers

Provides the details of the member servers in the domain.

To view the report, click the **Member Servers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Domain Controllers

Provides the details of the domain controllers in the domain.

To view the report, click the **Domain Controllers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Computer OS Based Reports

Computer OS Based Reports

- Computers by OS Service Pack

Computers by OS Service Pack

Provides the details of the computers based on the operating system and service pack versions.

To view the report, click the **Computers by OS Service Pack** available under OS Based Reports category. Select the Operating System and the Service Packs to filter the view. Clicking a computer account from the report displays the complete information of that account.

Active Directory Group Reports

Active Directory Group Report

To access the Group Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Group Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Group Reports provided by Desktop Central

- General Group Reports
- Group Type Reports
- Group Member Based Reports

Active Directory General Group Reports

Active Directory General Group Reports

- All Groups
- Recently Created Groups
- Recently Modified Groups
- Groups by OU

All Groups

Provides the details of all the groups of the domain.

To view the report, click the **All Groups** link available under the General Reports category. Clicking a group from the report displays the complete information of that group.

Recently Created Groups

Provides the details of all the groups that are recently created. This is determined based on the value contained in the *createTimeStamp* of the Active Directory.

To view the report, click the **Recently Created Groups** link available under the General Reports category.

By default, the groups created for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a group from the report displays the complete information of that group.

Recently Modified Groups

Provides the details of all the groups that are recently modified. This is determined based on the value contained in the *modifyTimeStamp* of the Active Directory.

To view the report, click the **Recently Modified Groups** link available under the General Reports category.

By default, the groups modified in the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a group from the report displays the complete information of that group.

Groups by OU

Provides the list of groups filtered by the OU it belongs to.

To view the report, click the **Groups by OU** link available under the General Reports category.

By default, the groups of all the OUs in the domain are listed. Browse to select a specific OU and click **Generate** to view the groups of that OU. Clicking a group from the report displays the complete information of that group.

Active Directory Group Type Reports

Active Directory Group Type Reports

- Security Groups
- Distribution Groups

Security Groups

Provides the details of the security groups available in the domain. This is determined based on the value contained in the *groupType* attribute of the Active Directory.

To view the report, click the **Security Groups** link available under the Group Type Based Reports category. Clicking a group from the report displays the complete information of that group.

Distribution Groups

Provides the details of the distribution groups available in the domain. This is determined based on the value contained in the *groupType* attribute of the Active Directory.

To view the report, click the **Distribution Groups** link available under the Group Type Based Reports category. Clicking a group from the report displays the complete information of that group.

Member Based Reports

Member Based Reports

- Groups with Member Details
- Groups with Maximum Members
- Groups without Members
- User-only Groups
- Computer-only Groups
- Nested groups

Groups with Member Details

Provides the details of the groups with its member count, such as no. of users, computers, groups, etc.

To view the report, click the **Groups with Member Details** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Groups with Maximum Members

Provides the details of the large groups in the domain based on its members count.

To view the report, click the **Groups with Maximum Members** link available under the Member Based Reports category. You can customize the report by selecting the member count. Clicking a group from the report displays the complete information of that group.

Groups without Members

Provides the list of groups that do not have any members.

To view the report, click the **Groups without Members** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

User-only Groups

Provides the list of groups that have only users as its members.

To view the report, click the **User-only Groups link** available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Computer-only Groups

Provides the list of groups that have only computers as its members.

To view the report, click the **Computer-only Groups** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Nested groups

Provides the list of nested groups (groups within groups) in the domain.

To view the report, click the **Nested groups** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Active Directory Organization Unit Reports

Active Directory Organization Unit Report

To access the Organization Unit Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **OU Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various OU Reports provided by Desktop Central

- Active Directory General OU Reports
- OU Child Based Reports

Active Directory General OU Reports

Active Directory General OU Reports

- All OUs
- Recently Created OUs
- Recently Modified OUs

All OUs

Provides the list of all the OUs of the domain.

To view the report, click the **All OUs** link available under the General Reports category. Clicking an OU from the report displays the complete information about that OU.

Recently Created OUs

Provides the list of OUs that are recently created. This is determined based on the value contained in the *createTimeStamp* attribute.

To view the report, click the **Recently Created OUs** link available under the General Reports category.

By default, the report displays the OUs created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking an OU from the report displays the complete information about that OU.

Recently Modified OUs

Provides the list of OUs that are recently modified. This is determined based on the value contained in the *ModifyTimeStamp* attribute.

To view the report, click the **Recently Modified OUs** link available under the General Reports category.

By default, the report displays the OUs modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking an OU from the report displays the complete information about that OU.

OU Child Based Reports

OU Child Based Reports

- OUs with Child Details
- OUs without Children
- User-only OUs
- Computer-only OUs
- Nested OUs

OUs with Child Details

Provides the list of OUs with its child details, like no. of users, computers, groups, and OUs.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

OUs without Children

Provides the list of OUs that do not have any children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

User-only OUs

Provides the list of OUs that have only users as their children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Computer-only OUs

Provides the list of OUs that have only computers as their children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Nested OUs

Provides the list of OUs that nested (OUs within OUs).

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Active Directory Domain Reports

Active Directory Domain Reports

To access the Domain Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Domain Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Domain Reports provided by Desktop Central

- Active Directory General Domain Reports
- Active Directory Container Reports

General Domain Reports

General Domain Reports

- Active Directory Sites
- Active Directory Domains
- Active Directory Printers
- Group Policy Creator Owners

Active Directory Sites

Active Directory Site Report provides the list of Sites with their attributes, such as Site name, subnet, netmask, and domain controller. Clicking a site from the report provides more details, such as the number of computers in each subnet, creation time, modified time, and so on.

To view the report, Click the **Active Directory Sites** link available under the General Reports category.

Active Directory Domains

Active Directory Domain Report provides the complete information of domain with the fully qualified Domain name, creation time, modified time, location, and its members.

To view the report, Click the **Active Directory Domains** link available under the General Reports category.

Active Directory Printers

Active Directory Printer Report provides the list of printers with their attributes such as name, host server name, model of printer, physical location and share name. Clicking the printer from the report gives details, such as Domain name, Active Directory URL, Model, Physical location, Share name, Modified time, Creation time, Printer Hosted Server name, Driver name, and Port name.

To view the report, Click the **Active Directory Printers** link available under the General Reports category.

Group Policy Creator Owners

Provides the members of Group Policy Creator Owners (GPCO) group. The members of this group can modify group policy for the domain.

To view the report, click the **Group Policy Creator Owners** link available under the General Reports category.

Container Based Reports

Container Based Reports

- Users In "Users" Container
- Groups In "Users" Container
- Computers In "Computer" Container
- Groups In "Builtin" Container

Users In "Users" Container

Provides the list of users in the "users" container of the domain.

To view the report, click the **Users In "Users" Container** link available under the Container Based Reports category.

Groups In "Users" Container

Provides the list of groups in the "users" container of the domain.

To view the report, click the **Groups In "Users" Container** link available under the Container Based Reports category.

Computers In "Computer" Container

Provides the list of computers in the "computer" container of the domain.

To view the report, click the **Computers In "Computer" Container** link available under the Container Based Reports category.

Groups In "Builtin" Container

Provides the list of groups in the "Builtin" container of the domain.

To view the report, click the **Groups In "Builtin" Container** link available under the Container Based Reports category.

Active Directory GPO Reports

Active Directory GPO Reports

To access the GPO Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **GPO Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various GPO Reports provided by Desktop Central

- General GPO Reports
- GPO Link Based Reports
- Inheritance Based Reports
- GPO Status Based Reports
- Special GPO Reports

General GPO Reports

General GPO Reports

- All GPOs
- Recently Created GPOs
- Recently Modified GPOs
- GPOs by OUs

All GPOs

Provides the list of GPOs that are created in the domain.

To view the report, click the **All GPOs** link available under the General Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Recently Created GPOs

Provides the list of GPOs that are recently created in the domain.

To view the report, click the **Recently Created GPOs** link available under the General Reports category. This is determined based on the value contained in the *createTimeStamp* attribute.

By default, the report displays the GPOs created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a GPO from the report displays the complete information about that GPO.

Recently Modified GPOs

Provides the list of GPOs that are recently modified in the domain. This is determined based on the value contained in the *ModifyTimeStamp* attribute.

To view the report, click the **Recently Modified GPOs** link available under the General Reports category.

By default, the report displays the GPOs modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a GPO from the report displays the complete information about that GPO.

GPOs by OUs

Provides the list of OUs and their linked GPOs.

To view the report, click the **GPOs by OUs** link available under the General Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPO Link Based Reports

GPO Link Based Reports

- GPOs Linked To OUs
- GPOs Linked To Domains
- GPOs Linked To Sites

GPOs Linked To OUs

Provides the list of GPOs that are linked to OUs in the domain. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To OUs** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs Linked To Domains

Provides the list of GPOs that are linked to domains. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To Domains** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs Linked To Sites

Provides the list of GPOs that are linked to sites. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To Sites** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Inheritance Based Reports

Inheritance Based Reports

- Block Inheritance enabled OUs
- Block Inheritance enabled Domains
- Enforced GPOs

Block Inheritance enabled OUs

Provides the list of OUs that are prevented from inheriting GPOs from any of its parent container. This is determined based on the value contained in the *gPOptions* attribute of the Active Directory.

To view the report, click the **Block Inheritance enabled OUs** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Block Inheritance enabled Domains

Provides the list of domains that are prevented from inheriting GPOs from any of its parent container. This is determined based on the value contained in the *gPOptions* attribute of the Active Directory.

To view the report, click the **Block Inheritance enabled Domains** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Enforced GPOs

Provides the list of GPOs that have the enforced flag set. Enforced GPOs when applied to OUs are also applied to their children irrespective of whether Block Inheritance is set or not.

To view the report, click the **Enforced GPOs** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPO Status Based Reports

GPO Status Based Reports

- User Settings Enabled GPOs
- Computer Settings Enabled GPOs
- User and Computer Settings Enabled GPOs
- Disabled GPOs
- Unused GPOs

User Settings Enabled GPOs

Provides the list of GPOs that have Computer Settings disabled. These GPOs can be used to make the user settings.

To view the report, click the **User Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Computer Settings Enabled GPOs

Provides the list of GPOs that have User Settings disabled. These GPOs can be used to make the computer settings.

To view the report, click the **Computer Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

User and Computer Settings Enabled GPOs

Provides the list of GPOs that can be used to perform both user and computer settings.

To view the report, click the **User and Computer Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Disabled GPOs

Provides the list of GPOs that have both User and Computer Settings disabled.

To view the report, click the **Disabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Unused GPOs

Provides the list of GPOs that are not used since creation.

To view the report, click the **Unused GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Special GPO Reports

Special GPO Reports

- GPOs with Most Modified User Settings
- GPOs with Most Modified Computer Settings
- GPOs with Most Modified User & Computer Settings

GPOs with Most Modified User Settings

Provides the list of GPOs that have user versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified User Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs with Most Modified Computer Settings

Provides the list of GPOs that have computer versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified Computer Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs with Most Modified User & Computer Settings

Provides the list of GPOs that have user or computer versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified User & Computer Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Custom Reports

While Desktop Central provides various canned reports on different modules like Patch Management, Asset Management, and so on, it is also possible to create customized reports to meet your specific requirement. Follow the links to learn more

- Wizard Based Custom Report
- Custom Query Report

Creating Custom Reports

In addition to the out-of-the-box reports, Desktop Central allows you to create custom reports by specifying the criteria and selecting the required parameters. Follow the steps below to create a custom report using Desktop Central:

1. Select the **Reports** tab from the Desktop Central Client.
2. Click the **New Custom Report** button available on the top-right. This opens the Custom Report page.
3. Specify the name for the report.
4. Select the Module. This is currently available only for the Asset Management module and will be extended for other modules in our subsequent updates.
5. Select the Sub Module as Computer, Hardware or Software.
6. Specify the criteria for generating the report. You can specify multiple criteria by clicking the "+" icon
7. Select the Columns to view in the report. You can change the position of the columns by using the up and down arrow icons.
8. Click on **Run & Save** button to save the report permanently. (or) Click **Run Report** if just a temporary report is needed.

   Note: If you choose the **Run Report** option, you can edit the report and later on save the same. Likewise if you intend to make any changes to a saved report, you can make use of the Edit option in the **Custom Report** Page.

9. You have an option to save this report as PDF and CSV formats.

Custom Query Report

Desktop Central provides the following types of reports:

- Canned reports on various modules like Patch Management, Asset Management, Active Directory, and so on.
- Wizard-based Custom Reports to retrieve any specific information

In addition to the above report types, it also provides an ability to retrieve the required information from the database using the Query Report. This might be useful in cases where you are not able to get the required information from the Canned or the Custom Reports.

The Query Report can be created using the **New Query Report** button available under **Reports tab --> Custom Report**. You may have to provide the SQL Query and create the report. The report can be saved for future reference and / or exported to CSV format for further processing.

From where can I get the Query?

Contact desktopcentral-support@manageengine.com with the details of your requirement. Alternatively, you can also submit your request online.

Our support team will process your requirement and send you the query.

Built-in Date Functions

Date is stored in the Long format in the database. You will not be able to interpret the date on seeing this long format. In order to convert this to readable date format, two built-n functions are included:

- LONG_TO_DATE() - for displaying the date in the results
- DATE_TO_LONG() - for using the date within the query

LONG_TO_DATE()

This function can be used to convert the date from the long value to the date format. Consider the following example:

You wish to retrieve software details along with the date and time at which the software was detected. The query you would normally use is:

```
Select SOFTWARE_NAME, DETECTED_TIME from invsoftware

SOFTWARE_NAME        DETECTED_TIME
Adobe Reader         1234558984892
Skype                8945934747893
```

In the above result, you will see the Detected Time in long format, which is not readable. Now, modifying the query as below will give you the desired output

```
Select SOFTWARE_NAME, LONG_TO_DATE(DETECTED_TIME) from
invsoftware

SOFTWARE_NAME        DETECTED_TIME_DATE_FORMAT
Adobe Reader         09/12/2009 15:35
Skype                07/13/2009  13.25
```

DATE_TO_LONG()

This function can be used to convert the Date format to Long value. Consider the example where you wish to retrieve the details of the software detected between two specific dates. You should use the query as below:

```
select * from invsoftware where DETECTED_TIME between
DATE_TO_LONG(08/01/2009 00:00:00) and
DATE_TO_LONG(08/31/2009 00:00:00)
```

The date should be specified in the following format: mm/dd/yyyy hh:mm:ss

Date Templates

For retrieving the data between some predefined dates, you can make use of the date templates. The following date templates are supported:

- Today - <from_today> - <to_today>
- Yesterday - <from_yesterday> - <to_yesterday>
- This Week - <from_thisweek> - <to_thisweek>
- Last Week - <from_lastweek> - <to_lastweek>
- This Month - <from_thismonth> - <to_thismonth>
- Last Month - <from_lastmonth> - <to_lastmonth>
- This Quarter - <from_thisquarter> - <to_thisquarter>
- Last Quarter - <from_lastquarter> - <to_lastquarter>

Making Help Desk Requests

The Users of the computers that are managed using Desktop Central can submit help desk requests from the Desktop Central Icon displayed in the system tray. Right-clicking the Tray Icon will display the following menus:

1. Send Request to Help Desk - to make a helps desk request
2. Apply User Configurations - to apply the configurations that are available for them.
3. Apply Computer Configurations - to apply the configurations that are available for all the users of that computer.
4. Scan and Upload Patch Details - to manually scan and update the server for Patch Management
5. Scan and Upload Inventory Details - to manually scan and update the server with software/hardware inventories.
6. View User Logon Reports - to view their login history.

Please note that the Administrator should have enabled these options for the users to view and use.

Appendix

This section includes the following topics:

- Interpreting Error Messages
- Knowledge Base
- FAQs
- Security Policies
- Windows System Tools
- Data Backup and Restore
- Dynamic Variables
- Limitations
- Glossary

Interpreting Error Messages

1. 1001: Storage Error Occurred
2. 1002: Unknown Error
3. 1003: DB Error
4. 1004: DB Error
5. 1010: Invalid User
6. 1011: User is already Inactive
7. 1101: Invalid container name
8. 1103: Group Policy Object (GPO) creation failed
9. 1104: Group Policy Object (GPO) deletion failed
10. 1105: Group Policy Object (GPO) linking failed
11. 1106: Group Policy Object (GPO) unlinking failed
12. 1107: WMI query failed
13. 1108: Active Directory error occurred
14. 1109: Unable to Extract Information from the given Msi Package
15. 1110: Access is Denied
16. 1111: File Copy Failed
17. 1112: Folder Copy Failed
18. 1113: The Given User Account is not a valid Domain Administrator
19. 1114: The Given Password is wrong
20. 1115: Active Directory/Domain Controller not Found
21. 1222: The Network is not present or not started

1001: Storage Error Occurred

The configurations defined using Desktop Central are stored in the database. If we are unable to store the configuration details, this error message is shown. The reasons could be any of the following:

- Could not establish connection with the database.
- Violations in data definitions.

1002: Unknown error

This error is shown when any runtime error occurs, which is not defined in Desktop Central. Please contact desktop central support with the details of the error.

1003: DB Error

This error is shown when the database connection is lost.

1004: DB Error

This error message is shown when you try to access the data, which has been deleted from the database.

1010: Invalid User

While defining the scope of management, if the user name provided is invalid, this error message is shown.

1011: User is already Inactive

When you try to add an user which is already present in the Inactive User list, this error message is shown.

1101: Invalid Container name

While defining targets for the configuration or while defining the scope of management, if an invalid / nonexistent container name is given this error occurs. The error message is shown, when you click Add more targets button or during deployment.

1103: Group Policy Object (GPO) creation failed

For every configuration a Group Policy Object (GPOs) will be created. When the GPO could not be created due to some access restrictions, etc., this error is shown.

1104: Group Policy Object (GPO) deletion failed

When an already defined configuration is deleted, the corresponding GPO is also deleted. This error is shown, when the GPO could not be deleted.

1105: Group Policy Object (GPO) linking failed

When a configuration defined, a GPO will be created and linked with the targets specified. This error is shown, when the linking fails.

1106: Group Policy Object (GPO) unlinking failed

When an already defined configuration is suspended, respective GPO will be unlinked from the targets. This error is shown, when the unlinking fails.

1107: WMI query failed

Desktop Central fetches the computer details through WMI. The WMI query may fail in the following cases:

1. Authentication failure
2. When the machine is shutdown
3. When the RPC server is not running.

1108: Active Directory error occurred

Pertains to the Active Directory related error. Please create a support file by clicking the **Support File** link available under the **Support** tab and send it to support@desktopcentral.com. Our support team will be able to assist you on this.

1109: Unable to Extract Information from the given Msi Package

The possible reason for this error could be that the MSI package is corrupted.

1110: Access is Denied

The Active Directory credentials are taken while you define the scope of management. This credential is stored in Desktop Central, which will be used for deploying configurations. When this credential becomes invalid or if it does not have necessary privileges, this error is shown.

One possible reason is that the credential is modified outside the Desktop Central.

1111: File Copy Failed

This error message is shown, when the user do not have necessary privileges to copy a file. Check whether the credentials supplied while defining the Scope of Management has necessary privileges.

1112: Folder Copy Failed

This error message is shown, when the user do not have necessary privileges to copy a folder. Check whether the credentials supplied while defining the Scope of Management has necessary privileges.

1113: The Given User Account is not a valid Domain Administrator

When the user account provided in the Scope of Management does not belong to a Domain Administrator group.

1114: The Given Password is wrong

The password provided in the Scope of Management is not valid.

1115: Active Directory/Domain Controller not Found

This error message is shown when no Active Directory/Domain Controller is found in your network. Desktop Central requires either of the two to perform the configurations.

1222: The network is not present or not started

This error message is shown when Desktop Central is unable to discover any domain. To fix this, start the Workstation service in the machine where Desktop Central is installed.

FAQs

1. What are the system requirements for Desktop Central?
2. What operating systems are supported by Desktop Central?
3. What is the difference between Free and Professional Editions?
4. Do I have to write scripts for using Desktop Central?
5. What is Scope of Management?
6. Do I need to define configurations separately or can I group them and define?
7. When are the configurations applied?
8. How to access Desktop Central UI or console from the remote ?
9. What is "Define Target"?
10. My free trial expired before I was through evaluating Desktop Central. Can I receive an extension?
11. Why is Desktop Central configuration done through a Web interface?
12. How is Desktop Central licensed?

1. What are the system requirements for Desktop Central?

Hardware Requirements for Desktop Central Server

No. of Computers Managed	Processor	RAM	Hard Disk Space
Upto 250 Computers	Single processor Intel P4 ~1.5 GHz	1 GB	2 GB*
251 to 500 Computers	Single processor (Intel P4 or Xeon 2.0 Ghz (Dual Core), 800+ Mhz FSB, 4 MB cache)	2 GB	2 GB*
501 to 1000 Computers	Single processor (Intel Xeon ~2.4 Ghz Dual Core, 800+ Mhz FSB, 4MB cache)	4 GB	3 GB*
1001 to 3000 Computers	Dual processor (Intel Xeon ~2.0 Ghz Dual Core, 1000 Mhz FSB,4 MB cache)	4 GB	5 GB*
3001 to 5000 Computers	Dual Processor (Intel Xeon processors Quad-Core at 2 ~ 3 GHz, 1000+ MHz FSB, 4 MB Cache)	6+ GB @ 667 Mhz. ECC	20 GB (HDD speed @ 7200 ~ 10,000 rpm)
5001 to 10000 Computers	Quad Processor (Intel Xeon processors Quad-Core at 2 ~ 3 GHz, 1000+ MHz FSB, 4 MB Cache)	8+ GB @ 667 Mhz. ECC	50 GB (HDD speed @ 7200 ~ 10,000 rpm)

Environment - Active Directory based Windows 2000/2003 domain setup.

Supported platforms - Windows 2000 Professional, Windows XP Professional, Windows Vista, Windows 7, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Virtual Servers (VM Ware)

Supported Browsers - IE 5.5 and above, Netscape 7.0 and above, Mozilla 1.5 and above. You must install and enable Java plugin to use the software.

2. What operating systems are supported by Desktop Central?

Desktop Central supports the following operating systems:

- Windows 2000 Professional
- Windows XP Professional
- Windows Vista
- Windows 7
- Windows 2000 Server
- Windows 2003 Server
- Windows 2008 Server
- Virtual Servers (VM Ware)

3. What is the difference between Free and Professional Editions?

While the free edition can be used to manage up to 25 desktops free of cost, the professional edition can be used to manage the number of desktops for which it is licensed for. The free edition can be upgraded to professional edition at any point of time by obtaining a valid license from ManageEngine.

4. Do I have to write scripts for using Desktop Central?

No, you do not have to write scripts for using any of the pre-defined configurations provided by Desktop Central. Just select the configuration, specify the required inputs, and deploy.

5. What is Scope of Management?

Scope of Management is used to define what are the computers to be managed using this software. When an Administrator use this software first time, he/she can use it with small set of computers then can slowly add more computers under management.

6. Do I need to define configurations separately or can I group them and define?

Configurations that are intended for the same set of targets can be grouped and defined as collections. However, when the targets differ, you have to define them separately.

7. When are the configurations applied?

1. All user configurations, except Custom Script configuration, are applied during user logon.
2. All computer configurations, except Custom Script configuration, are applied during system startup.
3. Custom Script configuration can be applied during user logon/logoff or system startup/shutdown.
4. Both user and computer configurations are applied every 90 minutes through Windows Group Policies.

8. How to access Desktop Central client or console from the remote?

To access the Desktop Central client from remote, open a supported browser and type http://<host name>:<port number> in the address bar,

where <host name> refers to the name / IP Address of the machine running Desktop Central,

<port number> refers to the port at which the product is started, the default being 8020.

9. What is "Define Target"?

Define Target is the process of identifying the users or computers for which the configuration have to be applied. The targets can be all users/computers belonging to a Site, Domain, OUs, Groups, or can be a specific user/computer. You also have an option to exclude some desktops based on the machine type, OS type, etc.

10. My free trial expired before I was through evaluating Desktop Central. Can I receive an extension?

Customer Satisfaction is our prime motive. During the trial period of 30 days, unlimited number of desktops can be managed by Desktop Central. After the trial period the Software automatically switches to the free edition where only 25 desktops can be managed.

If you feel you would like to test the software for more number of desktops, but your trial period has expired, Kindly contact us so that we can arrange for a temporary license for few more days as per your requirement. You may note that the transition is smooth with no data loss and the configurations are not lost at any point of time. We want to make sure you are completely satisfied that the software is satisfying your need and solving your problem before buying it.

11. Why is Desktop Central configuration done through a Web interface?

Desktop administrators are always on the move. Desktop Central, with its web-based interface, facilitates the administrators to access the product from anywhere in the network not requiring them to be glued at one place for managing the desktops using the product.

12. How is Desktop Central licensed?

Desktop Central is licensed on annual subscription based on the number of Desktop it would manage. You can get the Pricing for the specific number of desktops from our online store.

Security Policies

Using Desktop Central, you can define the security restrictions for the users and computers in the domain. This section provides you a brief description about the various security restrictions that can be applied using the product. Follow the links to learn more about the supported security policies under each category:

- Active Desktop
- Desktop
- Control Panel
- Explorer
- Internet Explorer
- Network
- System
- Task Scheduler
- Windows Installer
- Start Menu and Taskbar
- Microsoft Management Console
- Computer

Security Policies - Active Desktop

Desktop Central supports configuring the following security policies in Active Desktop category:

Security Policy	Description
Remove Active Desktop item from Settings menu	This setting will remove the Active Desktop options from Settings on the Start Menu.
Remove all desktop items	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places.
Restrict adding any desktop items	Prevents users from adding Web content to their Active Desktop.
Restrict deleting any desktop items	Prevents users from deleting Web content from their Active Desktop. This setting removes the Delete button from the Web tab in Display in Control Panel.
Restrict editing any desktop items	Prevents users from changing the properties of Web content items on their Active Desktop. This setting disables the Properties button on the Web tab in Display in Control Panel.
Restrict closing any desktop items	Restrict closing any desktop items. This setting removes the check boxes from items on the Web tab in Display in Control Panel.
Do not allow HTML wallpaper	Permits only bitmap images for wallpaper. This setting limits the desktop background ("wallpaper") to bitmap (.bmp) files.
Restrict changing wallpaper	Specifies the desktop background ("wallpaper") displayed on all users' desktops. This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation.
Enable active desktop	Enables Active Desktop and prevents users from disabling it. This prevents users from trying to enable or disable Active Desktop while a policy controls it.
Disable active desktop	Disables Active Desktop and prevents users from enabling it. This prevents users from trying to enable or disable Active Desktop while a policy controls it.
Prohibit changes	Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration. This is a comprehensive setting that locks down the configuration you establish by using other policies in this folder. This setting removes the Web tab from Display in Control Panel.
Allow only bitmapped wall paper	Permits only bitmap images for wallpaper. This setting limits the desktop background ("wallpaper") to bitmap (.bmp) files.

Security Policy	Description
Enable filter in Find dialog box	Displays the filter bar above the results of an Active Directory search. The filter bar consists of buttons for applying additional filters to search results.
Hide AD folder	Hides the Active Directory folder in My Network Places. The Active Directory folder displays Active Directory objects in a browse window.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Desktop

Desktop Central supports configuring the following security policies in Desktop category:

Security Policy	Description
Hide and disable all items on the desktop	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places.
Remove my documents icon on the desktop	This setting removes the My Documents icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box.
Hide my network places icon in desktop	Removes the My Network Places icon from the desktop.
Hide Internet explorer icon on desktop	Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar.
Prevent adding, dragging, dropping and closing the taskbar tool	Prevents users from manipulating desktop toolbars. If you enable this setting, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars on to or off of docked toolbars.
Prohibit adjusting desktop toolbar	Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars.
Don't save settings at exit	Prevents users from saving certain changes to the desktop.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Control Panel

Desktop Central supports configuring the following security policies in Control Panel category:

Security Policy	Description
Hide Accessibility Options Applet	Prevents access to the accessibility applet in control panel
Hide Add/Remove Hardware Applet	Prevents access to the Add/Remove Hardware Applet in control panel
Hide Add/Remove Programs Applet	Removes Add/Remove Programs Applet in control panel
Hide Client Services for Network Applet	Netware supporting client service applet will be removed from control panel
Hide Data Sources (ODBC) Applet	Removes open data base connection applet from control panel
Hide Date/Time Applet	Removes date/time applet in control panel
Hide Desktop Themes Applet	Removes desktop themes applet
Hide Display Applet	Removes display applet from control panel
Hide Games Controller Applet	Removes Games Controller Applet from control panel
Hide Internet Options Applet	Hide internet option applet
Hide Keyboard and Mouse Applet	Removes keyboard and mouse applet
Hide Network Connections Applet #1	Removes LAN connection 1
Hide Network Connections Applet #2	Removes LAN connection 2
Hide Mail Applet	Removes mail configuring applet from control panel
Hide Phone and Modem Options Applet (2000+)	Removes phone and modem options applet
Hide Power Options Applet	Removes power option from control panel
Hide Regional Options Applet	Removes regional options applet
Hide Scanners and Cameras Applet	Removes scanners and cameras applet
Hide Sounds and Multimedia Applet	Removes sounds and multimedia applet
Hide System Applet	Removes system applet
Hide Users and Passwords Applet	Removes users and passwords applet from control panel
Disable control panel	Disables all Control Panel programs. This setting prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items.

Security Policy	Description
Remove add/remove programs	Prevents users from using Add or Remove Programs. This setting removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus.
Hide change or remove programs page	Removes the Change or Remove Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page.
Hide add new programs page	Removes the Add New Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page.
Hide add/remove Windows components page	Removes the Add/Remove Windows Components button from the Add or Remove Programs bar. As a result, users cannot view or change the associated page.
Remove support information	Removes links to the Support Info dialog box from programs on the Change or Remove Programs page.
Hide appearance and themes page	Removes the Appearance and Themes tabs from Display in Control Panel.
Hide screen saver tab	Removes the Screen Saver tab from Display in Control Panel.
Hide settings tab	Removes the Settings tab from Display in Control Panel.
Password protect the screen saver	Determines whether screen savers used on the computer are password protected.
Prevent changing wall paper	Prevents users from adding or changing the background design of the desktop.
Remove display in control panel	Disables Display in Control Panel.
Browse the network to find the printers	If you enable this setting or do not configure it, when users click "Add a network printer" but do not type the name of a particular printer, the Add Printer Wizard displays a list of all shared printers on the network and invites users to choose a printer from among them.
Prevent addition of printers	Prevents users from using familiar methods to add local and network printers.
Prevent deletion of printers	Prevents users from deleting local and network printers. If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a setting prevents the action.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Explorer

Desktop Central supports configuring the following security policies in Explorer category:

Security Policy	Description
Remove folder options menu item from the tools menu	Removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the Folder Options dialog box.
Remove Shutdown from Start menu and task manager	Removes shutdown from the start menu and task manager dialog.
Remove File menu from Explorer	Removes the File menu from My Computer and Windows Explorer
Remove 'Map network drive' and 'Disconnect network drive'	Prevents users from using Windows Explorer or My Network Places to map or disconnect network drives.
Remove Context Menu in Shell folders	Removes context menus which appears while right clicking any folder in the explorer
Turn on classic shell	This setting allows you to remove the Active Desktop and Web view features. If you enable this setting, it will disable the Active Desktop and Web view.
Allow only approved Shell extensions	This setting is designed to ensure that shell extensions can operate on a per-user basis. If you enable this setting, Windows is directed to only run those shell extensions that have either been approved by an administrator or that will not impact other users of the machine.
Do not track Shell shortcuts during roaming	Determines whether Windows traces shortcuts back to their sources when it cannot find the target on the user's system.
Remove search button from Windows explorer	Removes the Search button from the Windows Explorer toolbar.
Hides the manage item on the Windows explorer context menu	Removes the Manage item from the Windows Explorer context menu. This context menu appears when you right-click Windows Explorer or My Computer.
Remove hardware tab	This setting removes the Hardware tab from Mouse, Keyboard, and Sounds and Audio Devices in Control Panel. It also removes the Hardware tab from the Properties dialog box for all local drives, including hard drives, floppy disk drives, and CD-ROM drives.
Remove DFS tab	Removes the DFS tab from Windows Explorer.
Remove UI to change menu animation setting	Prevents users from selecting the option to animate the movement of windows, menus, and lists. If you enable this setting, the "Use transition effects for menus and tooltips" option in Display in Control Panel is disabled.
Remove UI to change keyboard navigation indicator setting	When this Display Properties option is selected, the underlining that indicates a keyboard shortcut character (hot key) does not appear on menus until you press ALT.

Security Policy	Description
No 'computers near me' in My Network places	Removes the "Computers Near Me" option and the icons representing nearby computers from My Network Places. This setting also removes these icons from the Map Network Drive browser.
No 'Entire network' in My Network places	Removes the Entire Network option and the icons representing networked computers from My Network Places and from the browser associated with the Map Network Drive option.
Do not request alternate credentials	This setting suppresses the "Install Program As Other User" dialog box for local and network installations. This dialog box, which prompts the current user for the user name and password of an administrator, appears when users who are not administrators try to install programs locally on their computers.
Request credentials for network installations	This setting displays the "Install Program As Other User" dialog box even when a program is being installed from files on a network computer across a local area network connection.
Hide logoff menu item	This option removes Log Off item from the Start Menu. It also removes the Log Off button from the Windows Security dialog box.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Internet Explorer

Desktop Central supports configuring the following security policies in Internet Explorer category:

Security Policy	Description
Restrict using new menu option	Prevents users from opening a new browser window from the File menu.
Restrict using open menu option	Prevents users from opening a file or Web page from the File menu in Internet Explorer.
Restrict using Save As... menu option	Prevents users from saving Web pages from the browser File menu to their hard disk or to a network share.
Restrict on search customization	Makes the Customize button in the Search Assistant appear dimmed.
Restrict importing and exporting of favorites	Prevents users from exporting or importing favorite links by using the Import/Export Wizard.
Restrict using find files (F3) within browser	Disables using the F3 key to search in Internet Explorer and Windows Explorer.
Restrict using save as Web page complete format option	Prevents users from saving the complete contents that are displayed on or run from a Web page, including the graphics, scripts, linked files, and other elements. It does not prevent users from saving the text of a Web page.
Restrict closing of browser	Prevents users from closing Microsoft Internet Explorer.
Restrict full screen menu option	Prevents users from displaying the browser in full-screen (kiosk) mode, without the standard toolbar.
Restrict viewing source menu option	Prevents users from viewing the HTML source of Web pages by clicking the Source command on the View menu.
Hide favorites menu	Prevents users from adding, removing, or editing the list of Favorite links.
Restrict using Internet Options... menu option	Prevents users from opening the Internet Options dialog box from the Tools menu in Microsoft Internet Explorer.
Remove 'Tip of the Day' menu option	Prevents users from viewing or changing the Tip of the Day interface in Microsoft Internet Explorer.
Remove 'For Netscape Users' menu option	Prevents users from displaying tips for users who are switching from Netscape.
Remove 'Tour' menu option	Remove the Tour menu option.
Remove 'Send Feedback' menu option	Prevents users from sending feedback to Microsoft by clicking the Send Feedback command on the Help menu.
Restrict using 'Open in New Window' menu option	Prevents using the shortcut menu to open a link in a new browser window.
Restrict using 'save this program to disk' option	Prevents users from saving a program or file that Microsoft Internet Explorer has downloaded to the hard disk.

Security Policy	Description
Remove context (right-click) menus	Prevents the shortcut menu from appearing when users click the right mouse button while using the browser.
Hide the General Option Screen	Removes the General tab from the interface in the Internet Options dialog box.
Hide Security Option Screen	Removes the Security tab from the interface in the Internet Options dialog box.
Hide Content Option Screen	Removes the Content tab from the interface in the Internet Options dialog box.
Hide Connections Option Screen	Removes the Connections tab from the interface in the Internet Options dialog box.
Hide Programs Option Screen	Removes the Programs tab from the interface in the Internet Options dialog box.
Hide Advanced Option Screen	Removes the Advanced tab from the interface in the Internet Options dialog box.
Restrict changing home page settings	Prevents users from changing the home page of the browser. The home page is the first page that appears when users start the browser.
Restrict changing color settings	Prevents users from changing the default Web page colors.
Restrict changing link color settings	Prevents users from changing the colors of links on Web pages.
Restrict changing font settings	Prevents users from changing font settings.
Restrict changing language settings	Prevents users from changing language settings.
Restrict changing Cache settings	Prevents users from changing Cache settings.
Restrict changing history settings	Prevents users from changing history settings.
Restrict changing accessibility setting	Prevents users from changing accessibility settings.
Restrict changing Content Advisor settings	Prevents users from changing the content advisor settings.
Restrict changing certificate settings	Prevents users from changing certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers.
Restrict changing Profile Assistant settings	Prevents users from changing Profile Assistant settings.
Restrict changing AutoComplete clear form	Prevents Microsoft Internet Explorer from automatically completing forms, such as filling in a name or a password that the user has entered previously on a Web page.
Restrict changing AutoComplete save password form	Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.
Restrict using Internet Connection Wizard	Prevents users from running the Internet Connection Wizard.
Restrict changing connection settings	Prevents users from changing dial-up settings.
Restrict changing Automatic Configuration	Prevents users from changing automatic configuration settings. Automatic configuration is a process that

Security Policy	Description
settings	administrators can use to update browser settings periodically.
Restrict changing proxy settings	Prevents users from changing proxy settings.
Restrict changing Messaging settings	Prevents users from changing the default programs for messaging tasks.
Restrict changing Calendar and Contact settings	Prevents users from changing the default programs for managing schedules and contacts.
Restrict Reset Web Settings feature	Prevents users from restoring default settings for home and search pages.
Restrict changing Check if Default Browser setting	Prevents Microsoft Internet Explorer from checking to see whether it is the default browser.
Restrict changing any Advanced settings	Prevents users from changing settings on the Advanced tab in the Internet Options dialog box.
Restrict changing Automatic Install of IE components	Prevents Internet Explorer from automatically installing components.
Restrict changing automatic check for software updates	Prevents Internet Explorer from checking whether a new version of the browser is available.
Restrict changing showing the splash screen	Prevents the Internet Explorer splash screen from appearing when users start the browser.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Network

Desktop Central supports configuring the following security policies in Network category:

Security Policy	Description
Hide 'Entire Network' from Network Neighborhood	Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and My Network Places.
AlphaNumeric password	Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2 ,3 ...) characters.
Enable access to properties of RAS connections available to all users	Determines whether a user can view and change the properties of remote access connections that are available to all users of the computer.
Ability to delete all user remote access connection	Determines whether users can delete all user remote access connections.
Ability to enable/Disable LAN connections	Determines whether users can enable/disable LAN connections.
Ability to rename LAN	Determines whether users can rename LAN or all user remote access connections.
Prohibit access to properties of LAN	Determines whether users can change the properties of a LAN connection.
Prohibit access to properties of components of LAN	Determines whether Administrators and Network Configuration Operators can change the properties of components used by a LAN connection.
Prohibit access to the advanced settings item on the advanced menu	Determines whether the Advanced Settings item on the Advanced menu in Network Connections is enabled for administrators.
Prohibit access to the dial-up preferences item on the advanced menu	Determines whether the Dial-up Preferences item on the Advanced menu in Network Connections folder is enabled.
Allow configuration of connection sharing (User)	Determines whether users can use the New Connection Wizard, which creates new network connections.
Prohibit adding and removing components for a LAN or RA connection	Determines whether administrators can add and remove network components for a LAN or remote access connection. This setting has no effect on non-administrators. If you enable this setting the Install and Uninstall buttons for components of connections are disabled, and administrators are not permitted to access network components in the Windows Components Wizard.
Prohibit TCP/IP advanced configuration	Determines whether users can configure advanced TCP/IP settings. If you enable this setting, the Advanced button on the Internet Protocol Properties dialog box is disabled for all users (including administrators).

Security Policy	Description
Prohibit viewing of status for an active connection	Determines whether users can view the status for an active connection. The connection status taskbar icon and Status dialog box are not available to users (including administrators).
Remove 'make available offline'	Prevents users from making network files and folders available offline. This setting removes the "Make Available Offline" option from the File menu and from all context menus in Windows Explorer.
Sync offline files before logging off	Determines whether offline files are fully synchronized when users log off.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - System

Desktop Central supports configuring the following security policies in System category:

Security Policy	Description
Restrict using registry editing tools	Disables the Windows registry editors, Regedit.exe
Remove task manager	If this setting is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action.
Restrict using Lock Workstation	Prevents users from locking their workstation
Restrict Changing Password	Prevents users from changing the password.
Restrict using Passwords applet in Control Panel	Prevents users from changing the account password of local users through the password applet in control panel.
Restrict using Change Passwords page	Prevents users from accessing change password
Hide Background page	Prevents users using background page
Hide Remote Administration page	Removes remote administration page
Hide User Profiles page	Removes user profiles pages
Hide Device Manager page	Removes device manager page
Hide Hardware Profiles page	Prevents hardware profile page form being accessed
Don't display the getting started welcome screen at logon	Suppresses the welcome screen. This setting hides the welcome screen that is displayed on Windows 2000 Professional and Windows XP Professional each time the user logs on.
Download missing COM components	Directs the system to search Active Directory for missing Component Object Model components that a program requires.
Prevent access to registry accessing tools	Disables the Windows registry editors, Regedit.exe and Regedit.exe.
Run legacy logon scripts hidden	Windows 2000 displays the instructions in logon scripts written for Windows NT 4.0 and earlier in a command window as they run, although it does not display logon scripts written for Windows 2000. If you enable this setting, Windows 2000 does not display logon scripts written for Windows NT 4.0 and earlier.
Run logoff scripts visible	If the setting is enabled, the system displays each instruction in the logoff script as it runs. The instructions appear in a command window.
Run logon scripts synchronously	If the setting is enabled, Windows Explorer does not start until the logon scripts have finished running. This setting

Security Policy	Description
	ensures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.
Run logon scripts visible	If the setting is enabled, the system displays each instruction in the logon script as it runs. The instructions appear in a command window.
Do not process the legacy run list	If the setting is enabled, the system ignores the run list for Windows NT 4.0, Windows 2000, and Windows XP.
Do not process the runonce list	You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts. If you enable this setting, the system ignores the run-once list.
Create a new GPO links disabled by default	This setting creates all new Group Policy object links in the disabled state by default. After you configure and test the new object links, either by using Active Directory Users and Computers or Active Directory Sites and Services, you can enable the object links for use on the system.
Enforce show policies only	Prevents administrators from viewing or using Group Policy preferences. A Group Policy administration (.adm) file can contain both true settings and preferences. True settings, which are fully supported by Group Policy, must use registry entries in the Software/Policies or Software/Microsoft/Windows/CurrentVersion/Policies registry subkeys. Preferences, which are not fully supported, use registry entries in other subkeys.
Turn off automatic update of ADM files	Prevents the system from updating the Administrative Templates source files automatically when you open Group Policy.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Task Scheduler

Desktop Central supports configuring the following security policies in Task Scheduler category:

Security Policy	Description
Hide property pages	This setting removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview.
Prevent task run or end	Prevents users from starting and stopping tasks manually.
Prohibit drag and drop	Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder.
Prohibit new task creation	Prevents users from creating new tasks
Prohibit task deletion	Prevents user from deleting users from the scheduled tasks folder
Remove advanced menu	Prevents users from viewing or changing the properties of newly created tasks.
Prohibit browse	This setting removes the Browse button from the Schedule Task Wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Windows Installer

Desktop Central supports configuring the following security policies in Windows Installer category:

Security Policy	Description
Always install with elevated privileges	This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.
Prohibit rollback	This setting prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows Installer cannot restore the computer to its original state if the installation does not complete.
Disable media source for any install	Prevents users from installing programs from removable media.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Start Menu and Taskbar

Desktop Central supports configuring the following security policies in Start Menu and Taskbar category:

Security Policy	Description
Remove user's folder from the start menu	Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden. This setting is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu.
Remove links and access to Windows update	Prevents users from connecting to the Windows Update Web site.
Remove common program groups from start menu	Removes items in the All Users profile from the Programs menu on the Start menu.
Prohibit user from changing My Documents path	Prevents users from changing the path to the My Documents folder.
Remove My Documents from start menu	Removes the Documents menu from the Start menu.
Remove programs on settings menu	Prevents Control Panel, Printers, and Network Connections from running.
Remove network connections from start menu	Prevents users from running Network Connections.
Remove favorites from start menu	Prevents users from adding the Favorites menu to the Start menu or classic Start menu.
Remove search from start menu	Removes the Search item from the Start menu, and disables some Windows Explorer search elements. This setting removes the Search item from the Start menu and from the context menu that appears when you right-click the Start menu. Also, the system does not respond when users press the Application key (the key with the Windows logo)+ F.
Remove help menu from start menu	Removes the Help command from the Start menu.
Remove run from start menu	Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.
Add logoff to the start menu	Adds the "Log Off <username>" item to the Start menu and prevents users from removing it.
Remove logoff on the start menu	Removes the "Log Off <username>" item from the Start menu and prevents users from restoring it.
Remove and prevent access to the shutdown command	Prevents users from shutting down or restarting Windows. This setting removes the Shut Down option from the Start menu and disables the Shut Down button on the Windows Security dialog box, which appears when you press CTRL+ALT+DEL.

Security Policy	Description
Remove drag-and-drop context menu on the start menu	Prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. Also, it removes context menus from the Start menu.
Prevent changes to taskbar and start menu settings	Removes the Taskbar and Start Menu item from Settings on the Start menu. This setting also prevents the user from opening the Taskbar Properties dialog box.
Remove context menu for the taskbar	Hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons.
Do not keep the history of recently opened documents	Prevents the operating system and installed programs from creating and displaying shortcuts to recently opened documents.
Clear history of recently opened documents history on exit	Clear history of recently opened documents on exit.
Turn off personalized menus	Disables personalized menus. Windows 2000 personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently.
Turn off user tracking	Disables user tracking. This setting prevents the system from tracking the programs users run, the paths they navigate, and the documents they open.
Add 'run in separate memory space' check box to run dialog box	Lets users run a 16-bit program in a dedicated (not shared) Virtual DOS Machine (VDM) process.
Do not use the search based method when resolving shell shortcuts	Prevents the system from conducting a comprehensive search of the target drive to resolve a shortcut.
Do not use the tracking based method when resolving shell shortcuts	Prevents the system from using NTFS tracking features to resolve a shortcut.
Gray unavailable Windows installer programs start menu shortcuts	Displays Start menu shortcuts to partially installed programs in gray text. This setting makes it easier for users to distinguish between programs that are fully installed and those that are only partially installed.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Microsoft Management Console

Desktop Central supports configuring the following security policies in Microsoft Management Console category:

Security Policy	Description
Restrict user from entering author mode	Users cannot create console files or add or remove snap-ins. Also, because they cannot open author-mode console files, they cannot use the tools that the files contain.
Restrict users to the explicitly permitted list of snap-ins	All snap-ins are prohibited, except those that you explicitly permit. Use this setting if you plan to prohibit use of most snap-ins. To explicitly permit a snap-in, open the Restricted/Permitted snap-ins setting folder and enable the settings representing the snap-in you want to permit.
Restrict/permit Component services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Computer management snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Device manager snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Disk management snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Disk de-fragmentation snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Event viewer snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting

Security Policy	Description
	determines whether this snap-in is permitted or prohibited.
Restrict/permit Fax services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Indexing services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Internet Information Services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Local users and groups snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Performance logs and alerts snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Shared folders snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit System information snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Security Policy	Description
Restrict/permit Telephony snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit WMI control snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit System properties snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Group policy snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Group policy tab for active directory tool snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Administrative templates (computer) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Administrative templates (users) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Folder redirection snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Internet explorer maintenance snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Security Policy	Description
Restrict/permit Remote installation services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Scripts (logon/logoff) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Scripts(startup/shutdown) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Security settings snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Software installation (computer) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Software installation (user) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Computer

Desktop Central supports configuring the following security policies in Computer category:

Security Policy	Description
Disable ctrl+alt+del requirement for logon	Determines whether pressing CTRL+ALT+DEL is required before a user can log on.
Restrict CD-ROM access to locally logged-on user only	Determines whether a CD-ROM is accessible to both local and remote users simultaneously.
Restrict Floppy access to locally logged-on user only	Determines whether removable floppy media is accessible to both local and remote users simultaneously.
Prevent users from installing printer drivers	It prevents users from installing printer drivers on the local machine.
Prevent user from changing file type association	Disables the buttons on the File Types tab. As a result, users can view file type associations, but they cannot add, delete, or change them.

The policy descriptions are taken from Microsoft Help Documentation

Windows System Tools

- Check Disk Tool
- Disk Cleanup Tool
- Disk Defragmenter Tool

Check Disk Tool

The Check Disk tool creates a status report of the disk based on its file system. The errors in the disk is also displayed. It can also be used to correct the disk errors.

Desktop Central supports the following options to run the check disk tool:

- *Verbose*: Displays the name of each file in every directory as the disk is checked.
- *Quick Check*: This option is available only for the NTFS File system. Selecting this option will perform the check disk operation quickly by skipping the checking of cycles within the folder structure and by performing a less vigorous check of index entries.

See Also: Windows System Tools, Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Viewing Task History, Disk Defragmenter, Disk Cleanup

Disk Cleanup Tool

The Disk Cleanup utility helps to cleanup the unwanted filed in the disk to increase the free space.

Desktop Central cleans the windows system for the following:

- *Remove Active Setup Temp Folders*
- *Compress old files*
- *Remove content indexer*
- *Remove downloaded Program Files*
- *Remove internet cache files*
- *Remove memory dump files*
- *Remove Office setup files*
- *Remove offline files*
- *Remove web pages*
- *Remove old check disk files*
- *Empty recycle bin*
- *Remove remote desktop cache files*
- *Remove setup log files*
- *Remove old system restore positions.*
- *Remove Temporary files*
- *Remove temporary offline files*
- *Remove uninstall backup images*
- *Remove webclient and web publisher cache files*

See Also: Windows System Tools, Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Viewing Task History, Disk Defragmenter, Check Disk

Disk Defragmenter Tool

Adapted from Windows Help Documentation

Volumes become fragmented as users create and delete files and folders, install new software, or download files from the Internet. Computers typically save files in the first contiguous free space that is large enough for the file. If a large enough free space is not available, the computer saves as much of the file as possible in the largest available space and then saves the remaining data in the next available free space, and so on.

After a large portion of a volume has been used for file and folder storage, most of the new files are saved in pieces across the volume. When you delete files, the empty spaces left behind fill in randomly as you store new ones.

The more fragmented the volume is, the slower the computer's file input/output performance will be.

Desktop Central provides option to run the defragmenter tool on multiple machines simultaneously. It supports the following options:

- *Verbose*: Displays the complete analysis and defragmentation reports
- *Analyze*: Analyzes the volume and displays a summary of the analysis report.
- *Force Defragmentation*: Forces defragmentation of the drive regardless of whether it needs to be defragmented.

See Also: Windows System Tools, Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Viewing Task History, Check Disk, Disk Cleanup

Data Backup and Restore

Desktop Central stores all the configuration details, status of deployed configurations, User Logon Reports, Active Directory reports, etc., in the database. Backing up the data is necessary to prevent the data loss that may happen due to unforeseen circumstances.

- Manual Data Backup
- Scheduled Data Backup
- Data Restore

Manual Data Backup

Follow the steps given below to take a back up of the ManageEngine Desktop Central data manually:

1. Open a command prompt
2. Go to *<Install_Dir>/DesktopCentral_Server/bin* directory.
3. Execute the **backupDB.bat** as given below:
   backupDB.bat *<destination_directory>*

   For example, **backupDB.bat c:\DesktopCentralBackup**

The backup file will be created and stored in the specified location in date-time.zip format. An example of the backup file name: **061018-1635.zip**

Note: The MySQL database should be running prior to running the script. If Desktop Central is running, the database will also be running. If not, start the database using the **startDB.bat** located under the *<Install_Dir>/DesktopCentral_Server/bin* directory.

Scheduled Data Backup

Follow the steps given below to schedule the data backup:

1. Select the **Admin** tab
2. Click the **Database Backup** link available under the Tools category. This opens the Database Backup screen.
3. Specify the time for performing the backup operation. The time should be specified in hh:mm:sec format. The database will be backed up at this time everyday.
4. Select the number of backups to be maintained. The older ones will automatically be deleted.
5. Specify the location to store the backed up database.
6. Select the "*Notify when the database backup fails*" option and specify the email addresses if you want to be notified in cases of any failures. Please note that you should have configured your mail server settings to get notified.
7. Click **Save Changes**.

	Note: 1. The destination directory specified as the argument should be an existing directory. If you specify a nonexistent directory, the data backup will not happen. 2. The MySQL database should be running when the task is called. If Desktop Central is running, the database will also be running.

Data Restore

To restore the backed up data, follow the steps below:

1. Open a command prompt
2. Go to <*Install_Dir*>/*DesktopCentral_Server/bin* directory.
3. Execute the **restoreDB.bat** file as given below:

   restoreDB.bat <*backup file name*>

The back up file name has to be the .zip file from which you wish to restore the data. This will restore the data from the backup file.

	Note: 1. Desktop Central should be shutdown prior to restoring the data. 2. After restoration, the changes made after the backup date will not be available.

Dynamic Variables

Dynamic Variables are those that are replaced dynamically by Desktop Central while applying the configurations. As the name implies, the value of these variables are not the same for all the users/computers.

For example, to redirect the shortcuts of the start menu that are common for all the users to the system drive, you can use the dynamic variable **$SystemDrive**. This will be replaced by the corresponding system drive of that computer (like C, D, etc.) while deploying the configuration.

The table below lists the dynamic variable supported by Desktop Central:

Dynamic Variable	Description	Example Value of the Variable
$ComSpec	Specifies the path to the command interpretor	C:\WINNT\system32\cmd.exe
$HomePath	Refers to the home directory as defined in UMD/AD	\\JOHNSMITH\
$NtType	Role of NT/2000/XP computer	Server, Workstation
$OS	Short name of currently installed operating system	Windows_NT
$OSVersion	2000 & XP will report back as NT	Windows 2000
$OStype	2000 & XP will report back as NT	NT
$OsBuildNumber	Refers to the build number of the currently installed operating system	1381, 2195
$OsCsdVersion	Refers to the service pack of the currently installed operating system	Service Pack 4
$ProfileDirDU	Will be replaced by the full path of the "Default User" profile	C:\Documents and Settings\Default User
$ProfilesDir	Will be replaced by the full path of where user profiles are stored	C:\Documents and Settings
$ShellCache	Will be replaced by the path to current user's Temporary Internet Files shell folder	C:\Documents and Settings\JohnSmith\Local Settings\Temporary Internet Files
$ShellCookies	Will be replaced by the path to current user's Internet Cookies shell folder	C:\Documents and Settings\JohnSmith\Cookies
$ShellDesktop	Will be replaced by the path to current user's Desktop shell folder	C:\Documents and Settings\JohnSmith\Desktop

Dynamic Variable	Description	Example Value of the Variable
$ShellFavorites	Will be replaced by the path to current user's Favorites shell folder (also referred to as "IE Bookmarks").	C:\Documents and Settings\JohnSmith\Favorites
$ShellHistory	Will be replaced by the path to current user's History shell folder	C:\Documents and Settings\JohnSmith\Local Settings\History
$ShellMyPictures	Will be replaced by the path to current user's My Pictures shell folder	C:\Documents and Settings\JohnSmith\My Documents\My Pictures
$ShellNetHood	Will be replaced by the path to current user's Network Neighborhood shell folder	C:\Documents and Settings\JohnSmith\NetHood
$ShellPersonal	Will be replaced by the path to current user's Personal shell folder (also referred to as "My Documents")	C:\Documents and Settings\JohnSmith\My Documents
$ShellPrintHood	Will be replaced by the path to current user's Printer Neighborhood shell folder	C:\Documents and Settings\JohnSmith\PrintHood
$ShellPrograms	Will be replaced by the path to current user's Start Menu Programs shell folder	C:\Documents and Settings\JohnSmith\Start Menu\Programs
$ShellRecent	Will be replaced by the path to current user's Recent Documents shell folder	C:\Documents and Settings\JohnSmith\Recent
$ShellSendTo	Will be replaced by the path to current user's Send To shell folder	C:\Documents and Settings\JohnSmith\SendTo
$ShellStartMenu	Will be replaced by the path to current user's Start-Menu shell folder	C:\Documents and Settings\JohnSmith\Start Menu
$ShellStartup	Will be replaced by the path to current user's Start Menu Startup shell folder	C:\Documents and Settings\JohnSmith\Start Menu\Programs\Startup
$ShellTemplates	Will be replaced by the path to current user's Templates shell folder	C:\Documents and Settings\JohnSmith\Templates
$SystemDrive	Refers to the drive where OS files are located	C:
$SystemRoot	Will be replaced by the path to operating system folder	C:\WINNT
$TempDir	Will be replaced by the path to the temporary directory on the client	C:\Documents and Settings\JohnSmith\Local Settings\Temp
$WinDir	Will be replaced by the path to user's Windows folder (usually same as SystemRoot, exception would be a terminal server)	C:\WINNT

Limitations

1. When a site is chosen as the target for a user configuration, the status of the configuration will always be In Progress. This is because, it is not possible to get the exact user counts of individual sites.
2. When a user login to different computers in a domain, the status of the configurations defined for that user will reflect the status of the latest deployment.
3. When an already defined configuration is modified and re-deployed, the previous data will be overwritten and will not be shown in history reports.
4. Remote Shutdown Tool will not work for Windows 2000 computers.
5. Disk Defragmentation is not supported in Windows 2000 computers.
6. Shared and IP Printer configurations will not work in Windows Vista , Windows 2008 and Windows 7 computers

Known Issues

1. Printers shared in a Domain cannot be shared to computers in a Workgroup or vice-versa.
2. Redirecting folders between computers of different Domains or between a Workgroup and a Domain computer is not supported.
3. Software Installation will not work in the following cases:
    1. Package is in computer share of one Domain and you are trying to install it to a computer in another Domain.
    2. Package is in computer share of a Domain and you are trying to install it to a computer in a Workgroup or vice-versa.
    3. Package is in computer share of one Workgroup and you are trying to install it to a computer in another Workgroup.
4. In Custom Script configuration, Logoff and shutdown scripts cannot be executed.

Known Issues in deploying Configuration to Windows Vista Client Machines

1. When Security Policies are deployed to Windows Vista machines, the status will be shown as successful, but, the policies will not be applied.

Known Issues in Desktop Sharing

1. If the remote computer is shutdown using Remote Desktop Sharing, the viewer will not close by itself and has to be closed manually. It will display a blue screen showing a message "Meeting has stopped".

2. When connecting from Firefox/Flock browsers, Desktop Central Add-on (xpi) will be installed every time you access a remote computer using the Active X viewer. If you do not accept to install the xpi within 20 seconds, the remote service will be killed and you will not be able to access it. You have to close the viewer and have to connect again.
3. In Java viewer, Zoom In, Zoom Out, and Full Screen icons in the toolbar will not work.
4. When a remote connection is established, a message "You are now controlling the desktop" will appear. If you do not click OK within 20 seconds, the connection will close automatically. You have to close the viewer and have to connect again.

Glossary

- Site
- Domain
- Organizational Unit
- Group
- User
- Computer
- IP Address
- Group Policy Object (GPO)
- Client Side Extension (CSE)
- Define Target
- Scope of Management
- Inactive Users
- Collection
- Applicable Patches
- Latest Patches
- Missing Patches
- Missing Systems
- Affected Systems
- Informational Patches
- Obsolete Patches

This section provides the description or definitions of the terms used in Desktop Central.

Site

One or more well connected (highly reliable and fast) TCP/IP subnets. A site allows administrators to configure Active Directory access and replication topology quickly and easily to take advantage of the physical network. When users log on, Active Directory clients locate Active Directory servers in the same site as the user.

Domain

Domain is a group of computers that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.

Organizational Unit (OU)

An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a Group Policy object can be linked, or over which administrative authority can be delegated.

Group

A collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail.

Security groups are used both to grant access to resources and as e-mail distribution lists.

User

The people using the workstations in the network are called users. Each user in the network has a unique user name and corresponding password for secured access.

Computer

The PCs in the network which are accessed by users are known as computer or workstation. Each computer has unique name.

IP Address

The expansion of IP Address is Internet Protocol Address. An unique IP Address is provided for each workstation, switches, printers, and other devices present in the network for identification and routing of information.

Group Policy Object (GPO)

A Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users.

Client Side Extension (CSE)

Desktop Central installs an Windows-compliant agent or a Client Side Extension (CSE) in the machines that are being managed. This is used to get the status of the applied configurations from the targets.

Define Target

Define Target is the process of identifying the users or computers for which the configuration have to be applied. The targets can be all users/computers belonging to a Site, Domain, OUs, Groups, or can be a specific user/computer. You also have an option to exclude some desktops based on the machine type, OS type, etc.

Scope of Management

Scope of Management (SOM) is used to define the computers that have to be managed using this software. Initially the administrator can define a small set of computers for testing the software and later extend it to the whole domain. This provides more flexibility in managing your desktops using this software.

Inactive Users

In a Windows Domain there may be cases where the user accounts have been created for some machines but they remain inactive for some reasons. For example, users like Guest, IUSER_WIN2KMASTER, IWAM_WIN2KMASTER, etc., will never login. These user accounts are referred to as Inactive Users. In order to get the accurate configuration status of the active users, it is recommended that the Admin User add the inactive user

accounts in their domain so that these users (user accounts) may not be considered for calculating the status.

Collection

Configurations that are intended for the same set of targets can be grouped as a collection.

Applicable Patches

This is a subset of the patches released by Microsoft that affect your network systems / applications. This includes all the patches affecting your network irrespective of whether they are installed or not.

Missing Patches

This refers to the patches affecting your network that are not installed.

Latest Patches

This refers to the patches pertaining to the recently released Microsoft bulletins.

Missing Systems

This refers to the systems managed by Desktop Central that requires the patches to be installed.

Affected Systems

This refers to the systems managed by Desktop Central that are vulnerable. This includes all the systems that are affected irrespective of whether the patches have been installed or not.

Informational Patches

There maybe some vulnerabilities for which Desktop Central is not able to determine if the appropriate patch or work around has been applied. There could also be patches for which manual intervention is required. These are categorized as Informational Items. Remediation of these issues usually involves a configuration change or work around rather than a patch.

Obsolete Patches

These are patches that are outdated and have another patch that is more recently released and has taken its place (Superseding Patch). If these patches are missing, you can safely ignore them and deploy the patches that supersede them.

Some definitions are adapted from Microsoft Help Documentation.